BLOCKCHAIN AND THE LAW: A READER

Editor: Xingan Li

LLB, LLM, LLD, PhD, School of Governance, Law and Society, Tallinn University, Estonia

Toronto Academe Press

BLOCKCHAIN AND THE LAW: A READER

Editor: Xingan Li
LLB, LLM, LLD, PhD
Associate Professor
School of Governance, Law and Society
Tallinn University, Estonia

TORONTO ACADEME PRESS

Made in Canada

Title: BLOCKCHAIN AND THE LAW: A READER
First Edition, August 2016

ISBN 9780973981315 (PDF)

Publisher:
Toronto Academe Press
670 University Ave.
Charlottetown PE
C1E 1E3

Toronto Academe Press

COPYRIGHTS HOLDERS

PREFACE

The rise of blockchain has become a new challenge to conventional ideas, law and practice in many fields, such as financing, data protection, and transaction security. The purpose of this book is to provide a multifaceted reader on issues pertinent to blockchain and the law in a collection form. The targeted audience of this book is master and doctoral law students who are interested in expanding their research to innovative and multidisciplinary topics. While these articles are mostly available for free access, such a collection provides a better understanding of the string of ideas from technological, legal and social standpoints. The editor recognized and respected both optimistic views and critical reviews, taking them seriously within the scope of academic discussions, in which students will make judgments by themselves once they have acquired the knowledge, experience, and skill. The following paragraphs sketch a whole image of the contents based mainly on abstracts of these papers.

In the explorative study, “Analyzing the Bitcoin network: the first four years, Matthias Lischke and Benjamin Fabian examined the economy and transaction network of the decentralized digital currency Bitcoin during the first four years of its existence. In order to develop insights into the evolution of the Bitcoin economy during this period, the authors established and analyzed a novel integrated dataset that enriched data from the Bitcoin blockchain with off-network data such as business categories and geo-locations. Their analyses revealed the major Bitcoin businesses and markets. Their results also gave insights on the business distribution by countries and how businesses evolved over time. They also showed that there was a gambling network that featured many very small transactions. Furthermore, regional differences in the adoption and business distribution could be found. In the network analysis, the small world phenomenon was investigated and confirmed for several subgraphs of the Bitcoin network.

In "Bitcoins – a global perspective", Nishith Desai Associates examined legal aspects in relation to Bitcoin specifically and as corollary to cryptocurrencies generally and analyses transactions respecting Bitcoin in India.

In "Bitcoin blockchain for distributed clearing: a critical assessment", Robert Sams realized that there had been a dramatic increase in interest in the idea of using distributed consensus technology to facilitate the settlement of financial transactions. One strategy that has been advocated attempts to use the Bitcoin blockchain, running meta-protocols on top of that network, so that of-chain assets such as securities and property titles can leverage the same transaction protocol used by the endogenous on-chain cryptocurrency asset. The author explained Bitcoin's unique favor of distributed consensus algorithm (hash-based proof-of-work) and how it was motivated by a design goal of censorship-resistant digital cash. It was then shown that censorship-resistant consensus had no mechanism for enforcing the correspondence between blockchain reality and legal reality that of-chain assets required. The article suggested that the security of the Bitcoin network itself would be compromised by such an attempt.

Konrad S. Graf's paper, "Revisiting conceptions of commodity and scarcity in light of Bitcoin", examined Bitcoin using a typical set of criteria for explaining the historical-evolutionary strengths of metallic coins as media of exchange. The article tried to answer the question: How does Bitcoin fare on a representative list of criteria used to describe what gives certain types of market goods competitive advantages in a monetary role? It concluded by recalling the importance of applying realistic comparative methods and avoiding comparisons of real options against idealized imaginary versions of other options. The focus was on the perspective of individual actors and discrete marginal objects of action (both tangible and intangible "objects"). The author addressed technical-system, payment-network, and social-system perspectives in On the origins of Bitcoin: Stages of monetary evolution (October 2013) and his three-part Bitcoin Decrypted video lecture series (December 2013). These treatments build on the action-theory foundations developed in this article in keeping with the Misesean tradition of methodological individualism, in which systemic treatments of social phenomena were to remain rooted in action analysis.

In "New kids on the blockchain: how Bitcoin's technology could reinvent the stock market", Larissa Lee recognized that the Bitcoin was the first and most successful digital currency in the world. It polarized the news almost daily, with either glowing reviews of the many benefits of an alternative and international currency, or doomsday predictions of anarchy, deflation, and another tulip bubble. This article focused on the truly innovative aspect of Bitcoin — and that which had gone mostly unnoticed since its inception — the technological platform used to transfer Bitcoin from one party to another. This technology was called the Blockchain. The Blockchain eschewed a

bank or other intermediary and allows parties to transfer funds directly to one another, using a peer-to-peer system. This disruptive technology has done for money transfers what email did for sending mail — by removing the need for a trusted third party just as email removed the need for using the post office to send mail. If this technology could be used for peer-to-peer money transfers, why not extend the technology to accomplish other forms of transfers? Imagine selling a house or buying a car peer-to-peer. What about using the Blockchain technology to buy and sell stocks? Stocks exchanged completely peer-to-peer could resolve many of the issues facing the stock market today, including high frequency trading and short sales. This article developed a peer-to-peer stock market system, the legal implications of such a system, and how this system would fit in with current legislation and regulation.

In the article "The Bitcoin blockchain as financial market infrastructure: a consideration of operational risk", Angela Walch analyzed the usage of the term "blockchain" the street with every significant financial institution experimenting with this new technology. The author found that many had said that this remarkable innovation could radically transform our financial system, eliminating the costs and inefficiencies that plague our existing financial infrastructures, such as payment, settlement, and clearing systems. Venture capital investments were pouring into blockchain startups, which were scrambling to disrupt the "quadrillion"- dollar markets represented by existing financial market infrastructures. A debate raged over whether public, "permissionless" blockchains (like Bitcoin's) or private, "permissioned" blockchains (like those being designed at many large banks) were more desirable. Amidst this flurry of innovation and investment, this article inquired into the suitability of the Bitcoin blockchain to serve as the backbone of financial market infrastructure, and evaluated whether it was robust enough to serve as the foundation of major payment, settlement, clearing, or trading systems. Positing a scenario in which the Bitcoin blockchain did serve as the technology enabling significant financial market infrastructures, this article highlighted the vital importance of functioning financial market infrastructure to global financial stability, and described relevant principles that global financial regulators had adopted to help maintain this stability, focusing particularly on governance, risk management, and operational risk. The article then moved to explicate the operational risks generated by the most fundamental features of Bitcoin: its status as decentralized, open-source software. Illuminating the inevitable operational risks of software, such as its vulnerability to bugs and hacking (as well as Bitcoin's unique "51% Attack" vulnerability), uneven adoption of new releases, and its opaque nature to all except coders, the article argued that these technology risks were exacerbated by the governance risks generated by Bitcoin's ambiguous governance structure. The article then teased out the operational risks spawned by decentralized, open-source governance, including that no one was

responsible for resolving a crisis with the software; no one could legitimately serve as "the voice" of the software; code maintenance and repair might be delayed or imperfect because not enough time was devoted to the code by volunteer software developers (or, if the coders were paid by private companies, the code development might be influenced by conflicts of interest); consensus on important changes to the code might be difficult or impossible to achieve, leading to splits in the blockchain; and the software developers who "run" the Bitcoin blockchain seemed to have backgrounds in software coding rather than in policy-making or risk management for financial market infrastructure. The article concluded that these operational risks, generated by Bitcoin's most fundamental, presumably inalterable, structures, strongly undermined the Bitcoin blockchain's suitability to serve as financial market infrastructure.

In "Securities, intermediation and the blockchain – an inevitable choice between liquidity?" Philipp Paech identified that the practice of securities holding, transfer and collateral has significantly changed over the past 200 years – moving from paper certificates and issuer registers to an intermediated environment, and from there to computerisation and globalisation. These changes made transacting more efficient and thus rendered markets more liquid. However, the law has lagged behind and was itself an obstacle to efficiency because international securities transactions were subject to considerable legal uncertainty. The latest global market development, a cryptographic transfer process commonly called 'the blockchain', was the most recent efficiency-enhancing change. It offered a unique possibility to create a consistent legal framework for securities from scratch, on the basis of a legal concept that to some extent resembled bearer securities. This paper showed what the new international legal framework could look like, in the light of experience gained from earlier developments.

In "The false premises and promises of Bitcoin", Brian P. Hanley pointed out that, designed to compete with fiat currencies, Bitcoin proposes it was a crypto-currency alternative. Bitcoin made a number of false claims, including: Bitcoin could be a reserve currency for banking; hoarding equals saving; and that we should believe Bitcoin could expand by deflation to become a global transactional currency supply. Bitcoin's developers combined technical implementation proficiency with ignorance of currency and banking fundamentals.

Mircea Ploteanu and Oleg Stratulat explored into "the risks of Bitcoin use". They recognized that Bitcoin was a currency that existed only virtually and had appeared due to the global financial crisis and development of technologies. Cashless payments became more popular and in this context e-commerce has improved. There were Bitcoin perspectives in the banking system, by emphasizing analyzing the strengths and weaknesses of this currency and the point of view of

investors, central banks and commercial banks. Analysis could be used to improve electronic commerce and cashless payments in Moldova, where cash was still very widely used.

In "Beyond Bitcoin: issues in regulating blockchain", Trevor I. Kiviat reviewed that the buzz surrounding Bitcoin had reached a fever pitch. Yet in academic legal discussions, disproportionate emphasis was placed on Bitcoins (that is, virtual currency), and little mention was made of blockchain technology—the true innovation behind the Bitcoin protocol. Simply, blockchain technology solved an elusive networking problem by enabling "trustless" transactions: value exchanges over computer networks that could be verified, monitored, and enforced without central institutions (for example, banks). This had broad implications for how we transact over electronic networks. The article integrated current research from leading computer scientists and cryptographers to elevate the legal community's understanding of blockchain technology and, ultimately, to inform policymakers and practitioners as they consider different regulatory schemes. An examination of the economic properties of a blockchainbased currency suggested the technology's true value lay in its potential to facilitate more efficient digital-asset transfers. For example, applications of special interest to the legal community included more efficient document and authorship verification, title transfers, and contract enforcement. Though a regulatory patchwork around virtual currencies has begun to form, its careful analysis revealed much uncertainty with respect to these alternative applications.

In "The case for the regulating of Bitcoin mining as a security", Benjamin Akins, Jennifer L. Chapman and Jason Gordon also recognized that Bitcoin was rapidly increasing in use throughout the world. The process for introducing new Bitcoin into the system was known as "mining." Mining, which was instrumental to the Bitcoin system, involved the use of powerful computer systems and complex, computational algorithms to verify or validate prior Bitcoin transactions. The reward for successfully undertaking this process was the creation and award of new Bitcoin to the miner. Bitcoin mining has become a tedious and difficult process. The race to verify transactions, and thereby earn Bitcoin, necessitates more sophisticated processes for verification and greater computational power. Many Bitcoin miners banded together in groups called "pools" to create a powerful mining platform. Some miners invested time and effort to build or maintain a suitable computer system, while others passively provided money or other resources toward the creation of the mining system. Many such mining pools have grown to allow individuals to collectively contribute effort to the transaction verification process in exchange for an interest in the proceeds from the mining activity. The Bitcoin mining pool has largely escaped regulation. This paper argued that the mining pool should be regulated under the existing federal securities regulation regime.

Andres Guadamuz and Chris Marsden's paper, "Blockchains and Bitcoin regulatory responses to cryptocurrencies", examined Bitcoin from a legal and regulatory perspective, answering several important questions. The authors began by explaining what Bitcoin is, and why it matters. They described problems with Bitcoin as a method of implementing a cryptocurrency. The questions they sought to answer include: was it legal? What were the regulatory responses to the currency? Could it be regulated? They made clear why virtual currencies were of interest, how self-regulation had failed, and what useful lessons could be learned. Finally, they produced useful and semi-permanent findings into the usefulness of virtual currencies in general, blockchains as a means of mining currency, and the profundity of Bitcoin as compared with the development of block chain technologies. They concluded that though Bitcoin might be the equivalent of Second Life a decade later, so blockchains might be the equivalent of Web 2.0 social networks, a truly transformative social technology.

In "A bit of a problem: national and extraterritorial regulation of virtual currency in the age of financial disintegration", Isaac Pflaum and Emmeline Hatley recalled the recent development of virtual currencies, such as Bitcoin, as well as the computer networks that supported them, having opened new avenues for the unbanked to reduce transaction costs and gain access to capital without reliance on existing remittance networks or traditional, often foreign, banking institutions that were the primary focus of Basel III. This article illustrated theuse of Bitcoin as a virtual currency was just the beginning of what could become a larger trend towards disintermediation of the delivery of financial services more generally. To realize the full potential of this revolutionary technology, however, it was essential that a coherent regulatory approach be developed that will address abuses of the technology, including fraud, money laundering, and tax evasion, such as what has recently been brought to light in the Silk Road case. In the absence of coordinated international action, a robust extraterritorial application of the U.S. Criminal Code appeared to be the most viable option for the United States to shape the development of this technology as a legitimate complement to the international banking system. This article began with a discussion of what Bitcoin was, why it was important, and how it has been regulated to date in the United States and elsewhere. This was followed by a discussion, using the Silk Road case as a guide, of how the extraterritorial use of the U.S. Criminal Code provided a mechanism for regulating Bitcoin in the absence of a more coordinated international approach.

In "The blocks is hot: a survey of the state of Bitcoin regulation and suggestions for the future", Misha Tsukerman first examined the history of Bitcoin and the mechanics of the Bitcoin protocol and the blockchain in Part I. Part II then discussed some of the potential uses of Bitcoin, from its potential as a currency, to the use of the blockchain to track other property interests. Part III

examined some of risks associated with Bitcoin, from its use in online black markets, the consumer protection risks to users, and Bitcoin's potential as a tax evasion mechanism. Part IV analyzed the current regulatory environment for Bitcoin and Bitcoin's role in criminal litigation. Finally, Part V suggested policy changes to disclosure requirements and tax classifications to facilitate the broader adoption of Bitcoin as a currency by the general public.

Paul du Plessis' paper "The nature of decentralized virtual currencies: benefits, risks, and regulation" focused on Bitcoin, the first decentralized variation of virtual currency. In 2008 the Bitcoin white paper was published online by Satoshi Nakamoto, a pseudonymous person or likely a group people. The paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" proposed a "purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution [..] a system for electronic transactions without relying on trust. The open source Bitcoin software was released in January 2009, with an establishment of an exchange rate only on October 5, 2009 where 1 USD = 1,309 BTC. This initial value was calculated as the electricity exerted per Bitcoin generated.3 Since then, the system has grown to into a currency that was used for 60 – 80 thousand transactions per day, has a market capitalization of 5 billion USD, and trades 1 BTC = 380 USD. Regardless of the extreme volatility in the exchange rate, an increasing number of suppliers were now accepting Bitcoin as a means of payment for a myriad of goods and services. Adopters included large multinationals companies such as eBay Inc's PayPal service, Dell Inc. (multinational technology corporation), DISH Network (pay-TV provider), CheapAir (airline) and Expedia Inc. (online travel agency, hotel bookings). The objective of this paper was to provide a description of the technical nature of Bitcoin and the reason for its existence. With an understanding of the basic workings of this new payment system, we could draw comparisons to fiat currency, analyze the associated risks and benefits, and effectively discusses the current regulatory framework. The second chapter introduced money theory. To understand Bitcoin, we required a basic understanding of the origin of money and role states and financial institutions played in the acceptance of money. It was accepted that the core objective of central banks was securing the stability of the national economy (price stability), and thus the stable value of a currency through maintaining public trust in the currency. The Bitcoin protocol autonomously determined how new Bitcoins were created and the total possible number of Bitcoins was fixed. This precluded the possibility of state intervention its supply and thus, questioned the role of the state. The third chapter described and technical and economic nature of Bitcoin, drawing a comparison between its key properties to fiat currency systems. This chapter provided a translation of the technical aspects of Bitcoin system which must be understood before its regulation could discussed. The fourth chapter described the potential economic and conceptual benefits of

decentralized virtual currencies, followed by chapter five which identified risks arising from the use of virtual currencies. Risks would be categorized according to the bearer of the risk (users, nonuser market participants, financial integrity, etc.). Chapter six discussed the regulation of virtual currencies. The regulatory vacuum Bitcoin once existed in was swiftly getting filled with varying sentiment, while most countries adopt a permissive stance, others outright ban it. Regulation was required to safeguard parties within the virtual currency ecosystem from various risks that accompanies its use. Decentralized virtual currencies faced particularly challenging law enforcement predicaments because of their ability to disregard national borders while having no "owner" that controlled the system, thus systems like Bitcoin, could not be tied to any single jurisdiction. Chapter seven concluded by mentioning noteworthy future applications of distributed ledger technology, and argued that the inventions underlying Bitcoin might change the world for the better.

In "Bitcoin and money laundering: mining for an effective solution", Danton Bryans analyzed the effects of Bitcoin and analogous virtual currencies on anti–money laundering (AML) enforcement. Part I gave a brief primer on money laundering and virtual currencies. Part II offered a Bitcoin primer, which differentiated Bitcoin technology from traditional currencies and competing virtual currencies. Part III analyzed whether Bitcoin was legal to use or trade in the United States, using domestic and international adoption of Bitcoin for guidance. Part IV discussed whether current U.S. AML regulatory schemes encompassed the entirety of Bitcoin use, finding that it did not. Finally, Part V offered suggestions for a regulatory scheme encompassing Bitcoin and analogous virtual currency technologies. Ultimately, the author recommended regulating Bitcoin currency exchanges under existing AML regulation schemes instead of broadening statutory definitions to control all aspects of Bitcoin or analogous virtual currencies. Attempting to regulate parties other than currency exchanges in the Bitcoin network would prove too onerous from a cost-benefit analysis perspective.

Helsinki, Finland, 2 August 2016 Xingan Li

TABLE OF CONTENTS

future internet

MDPI

Article

Analyzing the Bitcoin Network: The First Four Years

Matthias Lischke and Benjamin Fabian *

Institute of Information Systems, Humboldt-Universität zu Berlin, Spandauer Str. 1, 10178 Berlin, Germany; matthias.lischke@googlemail.com
* Correspondence: bfabian@wiwi.hu-berlin.de; Tel.: +49-30-2093-5662

Academic Editor: Thomas Risse
Received: 4 October 2015; Accepted: 2 February 2016; Published: 7 March 2016

Abstract: In this explorative study, we examine the economy and transaction network of the decentralized digital currency Bitcoin during the first four years of its existence. The objective is to develop insights into the evolution of the Bitcoin economy during this period. For this, we establish and analyze a novel integrated dataset that enriches data from the Bitcoin blockchain with off-network data such as business categories and geo-locations. Our analyses reveal the major Bitcoin businesses and markets. Our results also give insights on the business distribution by countries and how businesses evolve over time. We also show that there is a gambling network that features many very small transactions. Furthermore, regional differences in the adoption and business distribution could be found. In the network analysis, the small world phenomenon is investigated and confirmed for several subgraphs of the Bitcoin network.

Keywords: bitcoin; blockchain; cryptocurrencies; electronic payment; network analysis; complex networks; graph analysis

---

1. Introduction

Bitcoin is an important electronic and decentralized cryptographic currency system proposed by Satoshi Nakamoto [1]. It is based on a peer-to-peer architecture and there is no need for a central authority or central bank to control the money supply within the system [2]. Bitcoin relies on a proof-of-work system to verify and authenticate the transactions that are carried out in the network. For further verification purposes all transactions are public [2]. On the high economic relevance of Bitcoin cf. a plethora of online press articles such as those at the website of *The Economist* [3].

In this article, we analyze the public transaction history of the first four years of Bitcoin with respect to economic and network aspects. We have chosen this time period in order to limit the amount of data to be analyzed and to have a specific time frame that can be compared with later analyses in future work. This period gives valuable insights into the birth of an important electronic currency. The objective is to investigate the evolution of the Bitcoin economy during this initial period by enriching the data from the public ledger with off-network data such as business categories and geo-locations. These novel analyses supersede some preliminary results [4], especially in the geographic dimension, give insights on the business distribution by countries and how businesses evolve over time in the network. The descriptive statistics reveal what the major Bitcoin businesses and markets are. Furthermore, regional differences in the business distribution could be found. In the network analysis, the small world phenomenon is investigated and is established for several subgraphs of the Bitcoin network. The analysis of the degree distribution and power law on the time, business, and country aggregation level reveals that large portions of the network follow a power law distribution and can be considered as scale-free networks. Moreover, further network characteristics will be investigated.

This paper is structured as follows. In Section 2, we will give an introduction into the technology of Bitcoin and the major entities and roles of this economy. In Section 3, related work is discussed.

Section 4 presents the methods used in our study, in particular the data collection and storage and the metrics from social network analysis and graph theory that are applied in the later analysis. The empirical data we collected, its structure and refinement are presented in Section 5. Section 6 presents the results of our investigation, starting with the business-related analyses before turning the focus to the network structure of Bitcoin transactions. Section 7 concludes the article with a discussion of limitations and an outlook on future work.

2. Bitcoin Technology and Economy

A Bitcoin can be defined as a chain of digital signatures. By transferring the electronic coin to the next user it gets digitally signed with a hash of the previous transaction and the public key of the next owner; adding these together to the end of the Bitcoin. The signatures can be verified by the payee to prove the chain of ownership [1].

To avoid inflation in the system, a unique feature of the currency is that it has a predetermined limited number of 21 million coins in circulation. Until that point, which might be reached around the year 2140, the money supply will increase at a certain rate [5]. To provide some sort of anonymity, direct personally identifiable information is omitted from the transaction. Therefore, the source and destination address are encoded in the form of public keys. Every public key that serves as a pseudonym has a corresponding private key which is stored in the electronic wallet. These are used to sign or authenticate any transactions. To become part of the peer-to-peer network, one needs to have a client software that runs either on the own device or as cloud service [6].

A node in the network will not accept multiple transactions using the same inputs. The nodes accept only the first transaction they receive and reject all subsequent. This is done to prevent double spending from malicious users and is part of the proof-of-work concept [5].

The main idea behind the proof-of-work system is to make it expensive for a single user or a group of users to rewrite the history of transactions once it has been accepted as definite. This should prevent malicious users from double spending their Bitcoins [6].

The solution that Nakamoto [1] proposed is the use of a timestamp server that takes the hash of a block of items, timestamps it, and widely publishes the hash. The proof of work involves using hash algorithms such as SHA-256 to find a specific value. The objective is to increment a nonce in the block until a value is found that results in a required number of zero bits. The average work to do so is exponential with the number of zero bits, but the result can be easily verified. There is a predetermined target difficulty that is updated for every 2016 blocks that have been generated. This ensures that the time it takes to generate one block is on average about 10 min. The block is only accepted by users if all transactions in it are valid and the Bitcoins have not been spent previously. Users show their acceptance by using the newly found hash in the "previous hash" section of the next block they attempt to generate; thus adding a new block to the chain. This chain is called the block chain or transaction log and contains the entire history of all transactions that have been carried out in the network [5].

The generation of blocks by users is called mining and is achieved through providing a certain amount of computation power to the network to solve the proof-of-work problem. The expending of computation power is rewarded when generating a block. There is competition to get the reward, and the more computation power a user or group possesses the better the chance to get it. The reward is predetermined and started at 50 BTC. It will decrease by half every 210,000 blocks. In that way new Bitcoins are introduced to the network. This procedure will continue until the predetermined final amount of 21 million Bitcoins is in circulation, around the year 2140.

Figure 1 shows a general overview of the Bitcoin economy with its major participants. Users can exchange their fiat currencies into Bitcoins via exchange platforms or local exchanges (1); withdraw money from recently introduced Bitcoin ATMs (2); store Bitcoins in an online wallet (3); use payment services in transactions with online merchants (4); pay with Bitcoins in local shops or bars (5); gamble with Bitcoins on various gaming platforms (6); incorporate transactions in a block, called mining (7); thus verifying the transactions and publish it to the network via the block chain (8).

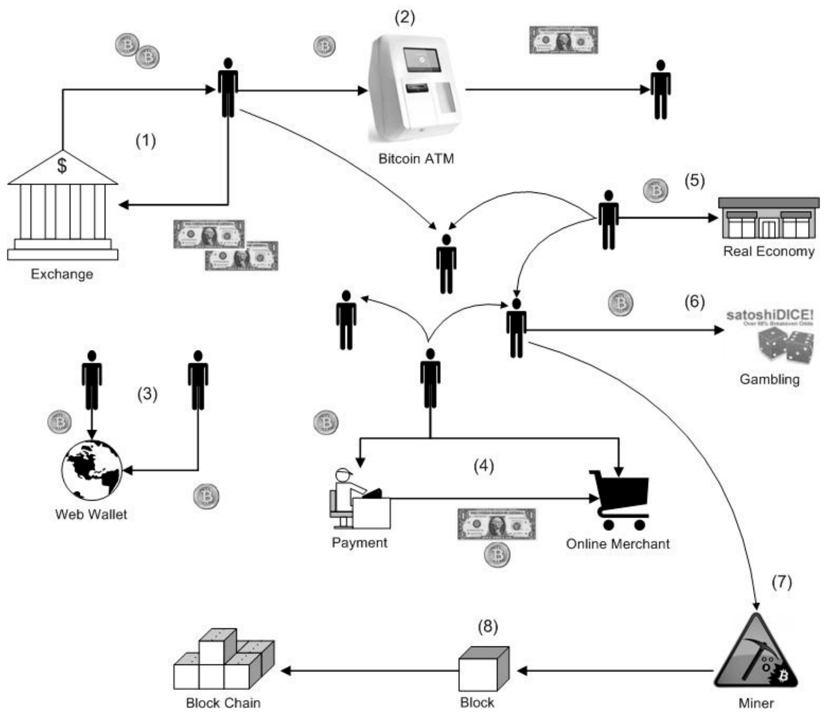


Figure 1. The Bitcoin Economy.

There is a vast amount of merchants and services that already accept Bitcoins as a currency in exchange for their offerings. The services can be mainly categorized into exchanges, wallets, mining, payments, gambling, and vendors.

- Exchanges: on exchanges one can trade their fiat currencies, other crypto currencies, and even gold into Bitcoins. The exchange platforms are mainly electronic but there are also local exchanges.
- Wallets: web wallets are similar to banks in the real economy where Bitcoins owned by users can be centrally stored on online platforms. The major advantage is that users can access their Bitcoins from every device connected to the web and have less effort to protect their wallet.
- Mining: mining is the contribution to the coin generation process, mainly executed in a mining pool. For a definition and comparison of mining pools see [7]. In such mining pools, miners share their computing resources and each participant receives a reward for the particular contribution of computing power.
- Payments: payment services enable online merchants to accept Bitcoins in the same way as they accept Visa or Paypal payments in their local currency. It reduces transaction costs, avoids chargebacks, Bitcoin exchanges rate risks, and identity thefts.
- Gambling: gambling services offer a wide variety of online games such as dice games, roulette, and other casino related games where users can gamble with their Bitcoins.
- Vendors: via online merchants users can exchange their Bitcoins for almost every kind of product such as multimedia content, electronics, travel, gift cards, clothing *etc.* There are also vendors that function as marketplaces such as Ebay.

The nature of Bitcoin services is quite unstable due to regulations or unsecure platforms that facilitate theft. The online merchant Silk Road was shut down because of trading illegal goods while the online wallet services MyBitcoin and Instawallet were closed due to several thefts [8].

3. Related Work

Most of the recent research focuses on the de-anonymization of Bitcoin users by introducing clustering heuristics to form a user network. To gain knowledge and get novel insights about the economic relationships between users this is an essential criterion. Furthermore, linking external information, relate to executed transactions, is an important step in analyzing the Bitcoin economy.

Reid and Harrigan [2] developed a clustering heuristic to form a user network by creating meaningful groups of users out of the vast amount of pseudonymous addresses (public keys) involved in transactions. The main idea is that multiple inputs of different public keys into a single transaction probably belong to the same user since the use of the corresponding private keys is highly coordinated. In order to construct the user network, all public keys that belong to the same user need to be clustered into one node or user entity. This user network represents the flow of Bitcoins between users over time. This clustering heuristic holds true if users do not share their private keys, but this is not always the case, for example in the case of web wallets that pool many private keys and would therefore mistakenly be clustered as a single user [9]. The clustering approach was extended by Androulaki *et al.* [10] who use another property in the Bitcoin protocol that is more complex but not that reliable in comparison to multi-input transactions. Since Bitcoins transacted from a single address need to be fully spent, the change is collected back to a newly generated address, the "shadow" or "change" address. In a transaction with two outputs, where one address has never appeared before in the block chain while the other address is public in the block chain, one can assume that the new address belongs to the user who initiated the transaction [10]. This approach is very reliable under the assumption that users rarely issue transactions to two different users. Pay-outs from mining pools or bets on gaming sites are examples where this is not always the case. Hence, Meiklejohn *et al.* [8] refined the clustering heuristics to account for these and other circumstances to increase the reliability.

Beside the clustering heuristics one want to add further information (e.g., IP addresses, geo-locations, businesses, and trade data from exchanges), which are related to transactions, to the user network. In their research Reid and Harrigan [2] also proposed several methods to overcome anonymity including the integration from off-network information such as email addresses, shipping addresses, IP addresses, or bank and credit card details. This information is mainly held by businesses that accept Bitcoin as payment and other services like exchanges, laundry services and mixers. The researchers use a number of publicly available sources and integrate their information with the user network. For instance, they scraped the web site Bitcoin Faucet over time and were able to associate IP addresses with the public keys involved in the transaction. Thus, they could plot a map of geo-located IP addresses belonging to users who received Bitcoins over a period of one week and overlay it with the user network.

Another approach of getting an IP address related to a transaction, was introduced by Kaminsky [11]. It exploits a leakage at the TCP/IP layer in the Bitcoin system. When a user is connected to every node in the peer-to-peer network, then the first node that publishes a transaction can be safely assumed the initiator of it; thus, the related IP address can be linked to that user [11].

Ortega [12] downloaded and analyzed the publicly available IP addresses related to transactions from the site Blockchain.info for a short time horizon. The data was then linked to public known IP addresses from anonymizing services such as Tor and Proxies. The results show that around one percent of transactions could be related to anonymizing services.

One more valuable source of identifying information is the voluntary disclosure of public keys by users on Bitcoin forums or other social network sites such as Twitter streams [2].

Meiklejohn *et al.* [8] gathered external data from various Bitcoin services such as gambling, mining, exchanges, and vendors to link it with public keys that interact with those businesses. Therefore they engaged in 344 transactions with a wide variety of different types of services. Another approach they propose is the collection from publicly available sources where users claim their own addresses. The site Blockchain.info provides the information in a convenient way via tagging the transactions with the associated business. With the collected data and the applied clustering heuristics they were able to classify a vast number of transactions in the user network [8].

Spagnuolo [9] introduced a tool called BitIodine that includes several external data from various sources such as Mt.Gox, Bitcointalk, and Blockchain.info in the analysis of the Bitcoin network. Through the APIs from Mt.Gox and Blockchain.info and several scrapers the researcher is able to gather most recent data about the transactions and the associated Bitcoin users [9].

Linking external information to transactions and subsequently to the formed user network gives meaningful insights in transaction flows and the overall Bitcoin economy.

4. Methods

Data management and network metrics for our study are introduced in the following.

4.1. Data Collection and Management

The Python 2.7 [13] based data scraper [14] builds the Bitcoin user network from the Bitcoin data files generated by the official Bitcoin client [15]. The programming and execution of the tool was conducted by Brugere [16] and is therefore out of scope in this work, but part of the complete architecture.

For gathering additional data from the websites blockchain.info and ipinfo.io, which are related to Bitcoin transactions, two Java-based data scrapers were programmed with the workbench Eclipse SDK [17]. The data was managed using an Oracle 11g database system.

NetworkX [18] is a Python based software package, which provides a large number of algorithms to analyze complex networks. It also comes with the functionality to visualize networks. Packages that can be used for visualization include MatPlotLib (PyLab) [19] or PyGraphviz [20], a Python interface to the Graphviz graph layout and visualization package. The tool is an essential part in analyzing the Bitcoin user network. Another powerful tool for network analysis, and especially for visualization of networks, is Gephi [21]. The tool will be used to visualize interesting subgraphs of the Bitcoin network.

The software environment Cran-R [22] is used for a wide area of statistical computing and graphics. We use it in our study for explorative spatial data analysis. This requires specific packages that can handle geographic data and are able to produce plots of maps. The general package for spatial data is [23]. For reading geographic data such as shape files the package maptools [24] is required. To visualize colored maps according to variables, the package RColorBrewer [25] is adopted.

4.2. Network Metrics

Several network metrics are used to analyze the structure and the dynamics of the Bitcoin network.

4.2.1. Degree Distribution and Power Laws

The degree distribution captures the structure of the network in terms of the individual connectivity of nodes. The degree of a node can be calculated for ingoing and outgoing connections as well as the total, *i.e.*, the sum of ingoing and outgoing connections of a node [26,27]. The degree distribution $P(k)$ gives the probability that a randomly selected node has exactly the degree k. In random networks the majority of nodes have approximately the same degree, close to the average degree $\bar{k}$ of the network; thus following a Poisson distribution with a peak at $P\left(\bar{k}\right)$ [28].

In contrast to random networks, real networks, such as social networks, the Internet, or citation networks, often follow a power law or scale-free distribution. The power law in terms of networks states that there are is a non-negligible number of highly connected nodes even though the majority of nodes are low connected. The probability that a new incoming node connects to an existing node is proportional to the degree k of that node; hence, becoming a scale-free network. This can be expressed in the form $P(k) \sim k^{-a}$ where a denotes a constant and k is the degree of a node in the network [29–31].

An important way for investigating the long tail of high degree nodes is to use the cumulative distribution function, which is the probability that the degree is greater than or equal to k.

$$\begin{aligned} P(k) &= \sum_{k'=k}^{\infty} P(k') \\ P(k) &\sim \sum_{k'=k}^{\infty} k'^{-a} \sim k^{-(a-1)} \end{aligned} \tag{1}$$

This has the advantage that all the original data is represented, in contrast to conventional histograms [30]. The cumulative distribution function $P(k)$ also follows a power law but with an exponent of $a - 1$, which is one less than the original exponent a. The most common way to estimate a is fitting a slope of the line in plots of the cumulative distribution [31]. Power law distributions can be found in many real networks. Newman [31] summarized several of them, such as word frequency, citations, telephone calls, web hits, or the wealth of the richest people. Barabasi, Albert and Jeong [32] have investigated this phenomenon for the World Wide Web and Inaoka *et al.* [33] for financial transaction networks.

4.2.2. Clustering

The clustering coefficient measures the network's transitivity. If a node A is connected to node B, and node B to node C, then there could be an increased probability that node A is also connected to node C. In the social network context this is described with: the friend of your friend is likely also your friend. In terms of network topology this reflects the presence of an increased number of triangles within the network [30]. A large number of networks show the tendency of such a formation between neighboring nodes in contrast to uncorrelated random networks. Equation (2) shows the formula for the local clustering coefficient (above) and for the average or global clustering coefficient (below).

$$\begin{aligned} C_i &= \frac{2T(i)}{k_i(k_i - 1)} \\ C_G &= \frac{1}{N}\sum_{i}^{N} C_i \end{aligned} \tag{2}$$

The local clustering coefficient C_i is defined as the number of triangles in which node i participates normalized by the maximum number of such triangles. $T(i)$ denotes the number of triangles through node i and k is the degree of node i. If $C_i = 0$ then none of the neighbors of a node are connected, and if $C_i = 1$ then all of the neighbors are connected.

The average clustering coefficient or global clustering coefficient C_G is the mean of all local coefficients C_i [34]. With the average clustering coefficient C_G one can measure the global cliquishness in the graph. Watts and Strogatz [35] introduced the clustering coefficient to graphs as part of discovering the small world phenomenon within networks.

4.2.3. Shortest Path Length

The Average Shortest Path Length is defined as the average number of steps along the shortest paths for all possible pairs of nodes and measures the efficiency of information or mass transport in the network. Examples are the number of average clicks to reach a website or the people one has to communicate through in a social network to contact a complete stranger.

The average shortest path length is defined as follows. In a network G with a set of nodes N the shortest distance between node i and j ($i, j \in N$) is defined as $dist(n_i, n_j)$. If $n_i = n_j$ or n_i cannot be reached from n_j then $dist(n_i, n_j) = 0$ and if $n_i = n_j$ or there is no path between n_i and n_j then

$has\_path\left(n_i, n_j\right) = 0$. With the existence of a path from n_i to n_j, $has\_path\left(n_i, n_j\right) = 1$ and the average shortest path length for network G ($ASPL_G$) can be calculated as shown in Equation (3) (top).

$$ASPL_G = \frac{\sum_{i,j}^{N} dist(n_i, n_j)}{\sum_{i,j}^{N} has\_path\left(n_i, n_j\right)}$$
$$ASPL_G = \sum_{i,j}^{N} \frac{dist\left(n_i, n_j\right)}{N\left(N-1\right)} \tag{3}$$

N denotes the number of nodes in network G, $\sum_{i,j}^{N} dist(n_i, n_j)$ is the value of all-pairs shortest path length of network G and $\sum_{i,j}^{N} has\_path\left(n_i, n_j\right)$ is the number of paths that exist in the network G. For a connected undirected graph $\sum_{i,j}^{N} has\_path\left(n_i, n_j\right)$ can be replaced by $N\left(N-1\right)$ as seen in Equation (5) (bottom), because paths exist between any pair of nodes [36].

The average shortest path length is used in combination with the average clustering coefficient to identify the small world phenomenon [35].

4.2.4. Centrality

Centrality measures the importance, influence or power of a node in the network and is widely applied in social network analysis. Important metrics have been introduced by Freeman [37]: degree centrality, betweenness centrality, and closeness centrality. Betweenness and closeness centrality count only geodesic paths, assuming that messages or transactions in a network flow only along the shortest possible paths. The eigenvector measure [38] counts walks, which assumes that trajectories can also revisit nodes and edges multiple times [39].

The degree centrality is based on the degree, *i.e.*, the number of links or direct connections that one node i has. To compare the degree centrality among networks of different size, one has to normalize by dividing the measure by the maximum possible number of adjacent connections, $N - 1$ (Equation (4), below).

$$C_D\left(n_i\right) = \sum_{i}^{N} a_{ij}$$
$$C\prime_D\left(n_i\right) = \frac{\sum_{i}^{N} a_{ij}}{N-1} \tag{4}$$

Nodes with higher degree centrality $C_D\left(n_i\right)$ or connections are more central to the network structure and tend to have more influence on others [37].

The betweenness centrality is based on the number of shortest paths passing through a node. Nodes with high betweenness play a central role in connecting different groups in a network. In Equation (5) $g_{jk}\left(i\right)$ is all geodesics linking node j and node k which pass through node i, and g_{jk} is the geodesic distance between node j and k.

$$C_B\left(n_i\right) = \sum_{j<k}^{N} \frac{g_{jk}\left(i\right)}{g_{jk}}$$
$$C\prime_B\left(n_i\right) = \frac{\sum_{j<k}^{N} \frac{g_{jk}\left(i\right)}{g_{jk}}}{\frac{1}{2}N\left(N-1\right)} \tag{5}$$

In social networks, nodes with high betweenness are the brokers and connectors that bring other groups in the network together. Nodes with the highest betweenness centrality measure result in the largest increase in a typical distance between others when they are removed [40]. The normalized version of the formula is shown in Equation (5) (bottom). It is normalized by the maximum number of pairs of nodes excluding the node itself [41].

The closeness centrality emphasizes the distance of a node to all other nodes in the network by focusing on the geodesic distance from each node to all others. Closeness centrality can be regarded as measure of how long it will take information to spread from a given node to others in the network. In Equation (6), $C_c(n_i)$ is the closeness centrality and calculated by the sum of the inverse distances $d(n_i, n_j)$ between two nodes in the network [40].

$$C_c(n_i) = \sum_{i}^{N} \frac{1}{d(n_i, n_j)}$$
$$C\prime_c(n_i) = \left[\sum_{i}^{N} \frac{d(n_i, n_j)}{N-1}\right]^{-1} \quad (6)$$

The node decentrality or inverse centrality grows when nodes are far apart, and centrality in this context means closeness. Information or other goods originated in the most central position of the network would spread throughout the network in minimum time. The most central node in the network is that with the minimum costs or time for communicating with all others. To remove the impact of the network size for comparability the formula is adjusted as seen in Equation (6) (bottom) [37].

The introduced centrality measures can be used to examine important hubs (degree) and brokers (betweenness) as well as to assess how efficiently information flows (closeness) within the network.

5. Data

The initial dataset that needs to be extracted is the Bitcoin transaction data, which is publicly available due to the proof-of-work concept for verification of transactions. This data can be scraped either from sites such as Blockexplorer.com or Blockchain.info, or by using a Bitcoin client that stores the entire transaction history (block chain). Secondly, additional data is scraped to enhance the dataset with meaningful information (e.g., IP, Geo, and Trade data) about transactions. In a third step, the data model is derived and loaded into the database. Figure 2 illustrates the data flow process.

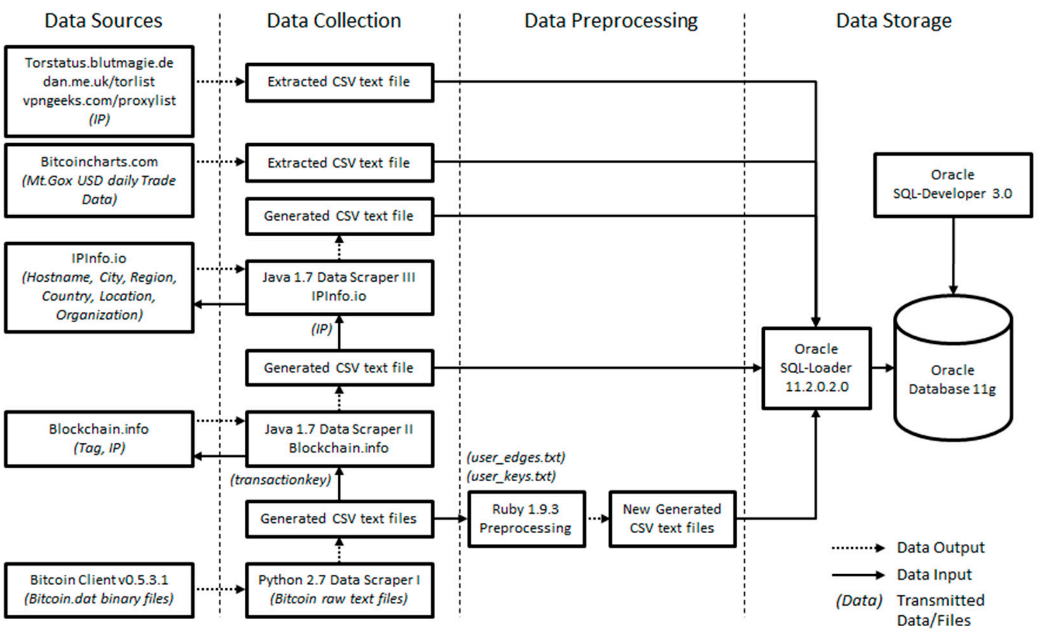


Figure 2. Data Flow Process.

5.1. Bitcoin Transaction Data

The transaction dataset that serves as a basis for this analysis was extracted from a full node Bitcoin client (version 0.5.3.1) with a Python 2.7 data scraper. The data scraper tool [42] from Brugere [16]

extends the Bitcoin tools developed by Martin Harrigan and Gavin Andresen. With these extensions it is possible to create the user network that was introduced by Reid and Harrigan [2]. The tool processes the Bitcoin.dat binary files that are part of the synchronized Bitcoin client software and transforms it into human readable raw text files as CSV. The first group of files, public_key.txt and transaction_key.txt contain the real hash values used in transactions within the Bitcoin network. With these values, additional information to the public key or the transaction can be retrieved from sites like Blockchain.info or Blockexplorer.com. The user information is organized by the second group of files (input_transaction_keys.txt, input_public_keys.txt, and user_keys.txt), where a "user" is a grouping of public keys that were used as inputs into a single transaction (user owns the private key to each address) as proposed by Reid and Harrigan [2]. Each line in user_keys.txt is a grouping of public keys as illustrated in Figure 3.

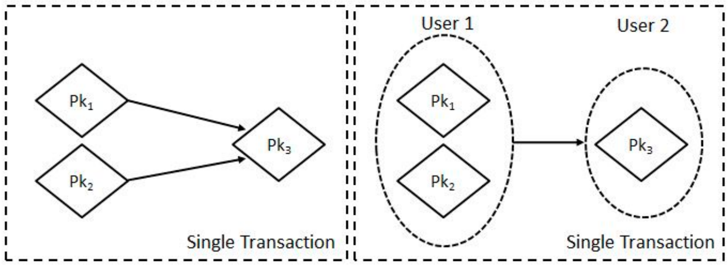


Figure 3. Forming the User Network.

The file user_edges.txt contains the primary network data, which includes the transaction key, the users (transaction from user_from to user_to) involved in this particular transaction, the time the transaction occurred in the block chain, and the transmitted value in Bitcoins of this transaction.

The initial data for this study originates from the data scraper execution by Brugere on the 10th April 2013 [16]. It contains 230,686 blocks and has the size of 1.51 GB, resulting in around 37.4 million edges and 6.3 million nodes.

Users can be seen as economic entities with a certain size determined by their number of public keys. The transactions between these economic entities are the relationships or edges in the network that come with additional properties. A simplified illustration of the entity network with nodes, edges, and their respective properties of the Bitcoin transactions are shown in Figure 4.

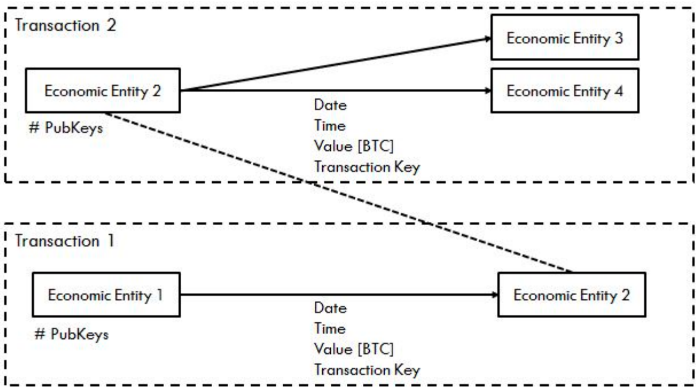


Figure 4. Bitcoin Entity Network.

5.2. Enriching the Dataset

To get more insight in the Bitcoin economy and the relationship between different entities and geographic regions, additional data related to transactions was scraped from several web sites.

The retrieved information included the IP addresses from the initiators of transactions, a Business tag related to that particular transaction, the geo-location information from the IP addresses, anonymous Tor IP addresses, and trade data from the Mt.Gox exchange.

5.2.1. IP and Business Tags

The most relevant information needed for this study is the IP address and the business tag from the initiator of a transaction. With the IP address one can derive information on how transactions are distributed geographically and generate aggregations based on country, region, or city level. Blockchain.info publishes the "relayed by" IP address which is derived with techniques introduced by Kaminsky [11], which means that the first node that informs about a transaction is, with high probability, also the source of it.

The tag for public key addresses is provided voluntary by the owner and can be used to categorize and aggregate transactions on different business levels such as gambling, mining, or exchanging. The IP addresses and tags, as well as other information, related to transactions are publicly available and can be accessed via a JSON API (JavaScript Object Notation) [43]. This technique makes the information accessible in a convenient way. The only parameter that is needed is the real transaction key. Since there are over 15.8 million transactions, an unlimited API access was requested and granted by the Blockchain.info administrator. The built Java scraper executes an URL request with the required parameter and retrieves the data from the JSON format via regular expressions (java regex). With "rawtx" one gets all available information to a single transaction in JSON format, such as the block height, the transacted values and the public keys involved.

Around 400 thousand transactions and their respective IP and tag data could be retrieved per day; thus, it took over 40 days to scrap the entire data from Blockchain.info.

5.2.2. IP Geo-location

With the previously scraped IP addresses one can derive additional information about the geo location, hostname, or the organization that is related to the IP. The site ipinfo.io provides all this information in the JSON format and can be accessed with an API, in the same way as Blockchain.info. Therefore, a second java scraper was built to retrieve the data from ipinfo.io. The database query resulted in over 223 thousand distinct IP addresses used in around 15.8 million transactions.

5.2.3. Tor and Proxy Nodes

To obfuscate the IP address from transactions, some users adopt anonymous proxies, VPNs, or Tor. For the geo-location of IP addresses and their respective economic entities one has to identify transactions that were executed via the Tor network, because one cannot surely determine the location based on these IP addresses. Therefore, all current Tor server and Tor server exit node IP addresses were downloaded as CSV files from the site torstatus.blutmagie.de. Another site that provides a list of Tor servers is dan.me.uk/torlist, where an additional list of IP addresses was extracted. Besides the Tor network, there are other proxy services that can be used; hence, IP addresses from known proxy servers were extracted from the site vpngeeks.com/proxylist. Subsequently, a combined list of Tor and proxy IP addresses was created that contains around 960 Tor exit nodes, 11,000 Tor servers, and 950 proxy servers.

5.2.4. Trade Data

The trade data from one of the most liquid exchange platforms for Bitcoins give insights on the money in- and outflows of the Bitcoin economy. To get an appropriate time horizon according to the network data and an exchange rate of the preferred currency used in the economy, the trading platform Mt.Gox and the exchange rate BTC/USD were chosen. The site bitcoincharts.com [44] provides historical trading data from the BTC/USD exchange rate for the chosen time horizon 17th July 2010 to 23rd December 2013. The data contain the trading date, open, high, low, and close price, the trading

volume in BTC and USD, and the weighted price. To analyze a particular trading day or special trades more thoroughly, the granularity can be adjusted down to one minute if preferred.

5.3. Final Data Model

After extracting data from several web sites, one has to incorporate it into a data model that can be used for further analyses and aggregations. Figure 5 shows the final data model for this study that contains all relevant information. Model and data are loaded into the Oracle 11g database. The central table is the Bitcoin transaction network, which is enriched by transaction-related data.

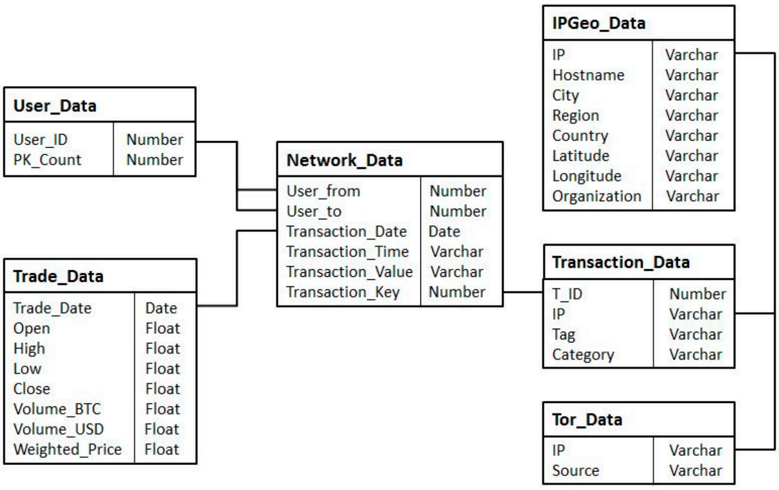


Figure 5. Final Data Model.

6. Analysis and Results

In this section, the analyses on the previously introduced final data model are conducted. Several aggregations on the business category, geo-location and time level will be examined to get a thorough insight into the Bitcoin economy. Furthermore, the network metrics will be applied to analyze the structure of the Bitcoin economy and identify important hubs, clusters, brokers, and to investigate the existence of the small world phenomenon within the network.

6.1. Statistics

6.1.1. Bitcoin General Statistics

Table 1 comprises some general descriptive statistics of the network data. In the time from 3rd January 2009, when the first transaction was carried out, until the 10th April 2013, around 6.3 million user entities were engaged in over 15.8 million transactions in the Bitcoin network. Since users can spend Bitcoins with different amounts to many other nodes, the entire network has over 37.4 million relationships. Hence, the Bitcoin economy can be seen as a large-scale transaction network.

Table 1. Descriptive Statistics of the Bitcoin Network (on daily bases).

	Median	Mean	Sd	Skew	Min	Max	Correl [EXRate]
Transaction Value [BTC]	173,457	910,053	2,231,647	7	50	29,958,714	0.199
Number of Users	1637	4049	5243	2	1	36,120	0.730
Number of Transactions	3678	24,084	38,303	2	1	189,284	0.680

Dataset: 03.01.2009–10.04.2013; Transactions (Relations): 37,450,461; Economic Entities (Nodes): 6,336,769.

The statistics of the Bitcoin network were aggregated on a daily bases. The transaction value ranges from a minimum of 50 BTC (initial transaction) to almost 30 million BTC per day, which

was reached on the 19th September 2012. The low median and mean as well as the high skewness indicate that the majority of executed transactions have very low values. On the 9th April 2013, the number of active users reached its peak (36,120) and can be related to the speculation hype at this time, resulting in a new record high on the exchange rate with around 201 BTC/USD. The highest number of transactions (189,284) on the network occurred in the same time horizon and was reached on the 3rd April 2013. The distributions of users and transactions indicate a rather low activity on an average daily bases in the network according to the statistics.

To examine the relationship between the user activity and the trading behavior on exchanges (here Mt.Gox as a representative), the time series of the trading volume and the exchange rate from Mt.Gox are compared to the user activity with different rolling windows over time. There is a strong relationship between the user activity and the exchange rate when considering the correlation coefficients in Table 2. Although there is a positive relationship of activity in the network to the trading behavior, the correlation to the trade volume is rather low. This indicates that a majority of users might not be active in the exchange business and therefore have no relationship to the traded volume. Another point is that the volume is not separated into buys and sells; hence, the correlation coefficient between the exchange rate and the volume is 0.22. In Figure 6, one can see that peaks in the exchange rate are followed by an increase in user activity; thus giving sign for high interest and speculative behavior in the Bitcoin economy. The relationship between user activity and trading behavior is very close to the actual exchange rate movements, as can be seen by the correlation coefficients for the 1 day and 10 days rolling window.

Table 2. Correlation Matrix (User Activity and Trade Behavior).

Trade Measure	User Activity (Rolling Windows)			
	1 Day	10 Days	30 Days	100 Days
BTC/USD	0.718	0.687	0.639	0.604
Volume	0.292	0.267	0.252	0.241

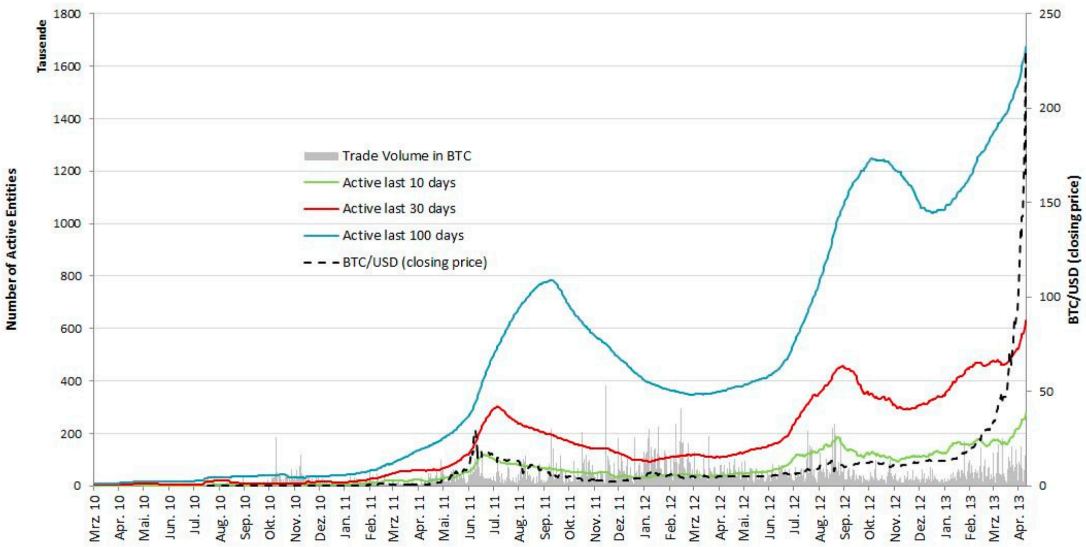


Figure 6. User Activity and Trade behavior.

One can conclude that there is a strong positive relationship between the user activity and the trading behavior but a rather low correlation to the trade volume. The overall user activity in the network increases steadily over time.

6.1.2. Bitcoin Business Statistics

The combined analysis of Bitcoin transactions and their associated businesses categories requires the classification of the extracted business tags. Since there are 1704 different tags which would need a manual lookup, the classification was done on tags that have ten or more transactions. This resulted in 383 tags that were classified in 13 different categories as shown in Table 3.

Table 3. Business Tags.

Category	Content	Examples	# Transactions	in %
Gambling	Dice & Casino Games	SatoshiDice, Betcoins	7,615,051	47.90%
Mining	Mining Pools & Services	Deepbit, ASICMiner	689,231	4.34%
Exchanges	Exchange Platforms	Mt.Gox, Bitcoin-24	293,969	1.85%
Wallets	Web Wallets and Clients	Instawallet, Strongcoin	17,748	0.11%
IT	Programming & Hardware Services	Free Software Foundation	4515	0.03%
Media News	Blogs, Media Channels, News	Wikileaks, Archive.org	7563	0.05%
Vendors	Selling Goods	Room77, Silk Road	2233	0.01%
Donation	Charity & other Donations	Faucet Donation	30,612	0.19%
Bitcoin Services	Sites offering Information & Services	Blockexplorer, Bitcoinmonitor	1420	0.01%
Bitcoin OTC	Over the Counter (OTC) Trader	DPP_, Eleuthria	5054	0.03%
Bitcoin Talk	Bitcoin Forum Users	Quip, Nikkos	3534	0.02%
Misc.	Free BTC Sites & Advertising	CoinAd, Hashluck	4123	0.03%
Unknown	Not Classified Transactions	n.a.	7,223,572	45.44%
Total	-	-	**15,898,625**	100%

Overall, 54.56% of all transactions could be categorized. With 47.90%, the largest portion of it contains gambling services followed by mining and exchanges. Because leaving out business tags with fewer than 10 transactions, 5151 or 0.032% are not categorized.

To give insights into the major businesses in the Bitcoin economy and how they are distributed among the categories, statistics over the top 25 businesses were taken. Although 54.56% of transactions are categorized, the gambling business SatoshiDICE alone comprises 46.9% of them; the mining pool Deepbit is associated to 4.3% of all transactions; and the exchange platform Mt.Gox comprises around 1.7% of transactions. Since it is clear that these three services incorporate over 52.9% of all transactions, they are excluded from the first statistics to get a better view and comparison on the other businesses in the economy.

Figure 7 shows the number of transactions, their value in BTC, and their distribution among categories (inset) of the top 25 businesses. The statistic comprises around 1.5% (236,747 TXs) of all transactions after excluding SatoshiDICE, Deepbit, and Mt.Gox. One can see that gambling services (67.4%) are by far the most active businesses in the economy. Donations are the second largest business group and account for 12.6% of transactions. When comparing the number of transactions and the associated value one recognizes that the value in the business category gambling (e.g., BTC Dice, DICEonCRACK, Bit Elfin) is abnormally low. The opposite is the case for the business category exchanges (e.g., Bitcoin-24, MPEx), where the value is abnormally high in comparison to the number of transactions.

For comparison reason a similar statistic was conducted with the focus on the transacted value in BTC. Figure 8 shows a completely different distribution of the top 25 businesses among the categories when considering the transaction value. The largest business category is exchanges that comprise 48.8% of transacted volume followed by the vendor business with 18.7%.

Especially the vendor Silkroad shows a large trading volume of around 1.23 million BTC in comparison to 285 executed transactions. In contrast, the gambling businesses transact very small Bitcoin volumes while a huge amount of transactions are executed. From a business view this makes sense that exchanges and vendors transact larger volumes because of transaction costs and reasonable prices for traded goods. On the other hand, risky gambling activities and donations incorporate rather small volumes per transaction.

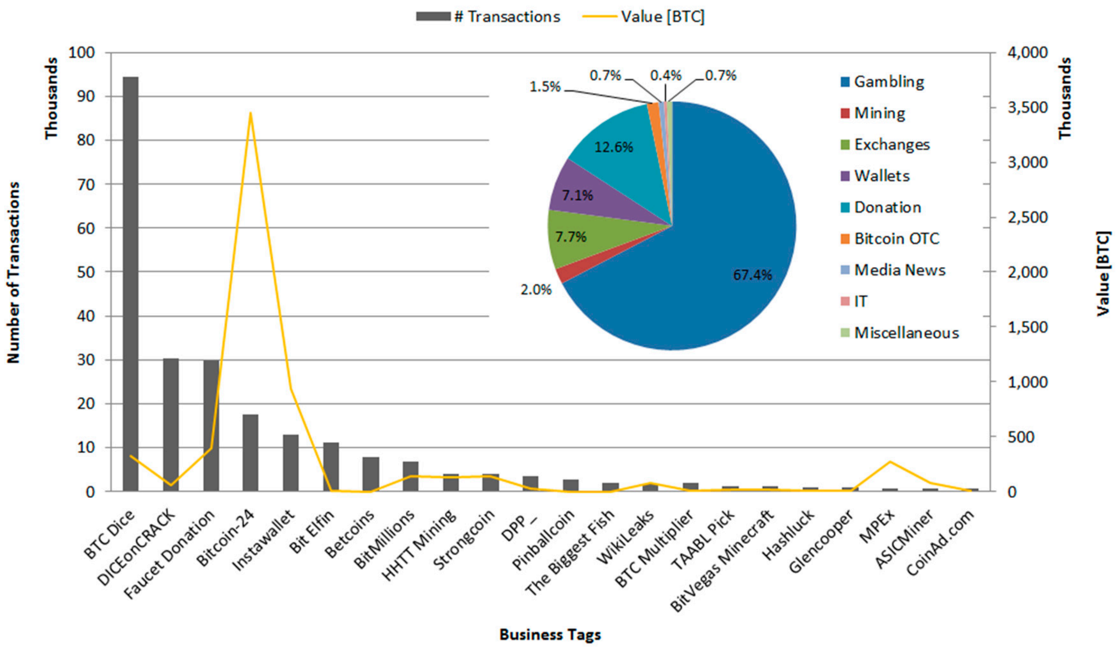


Figure 7. Top 25 Businesses (# Transactions).

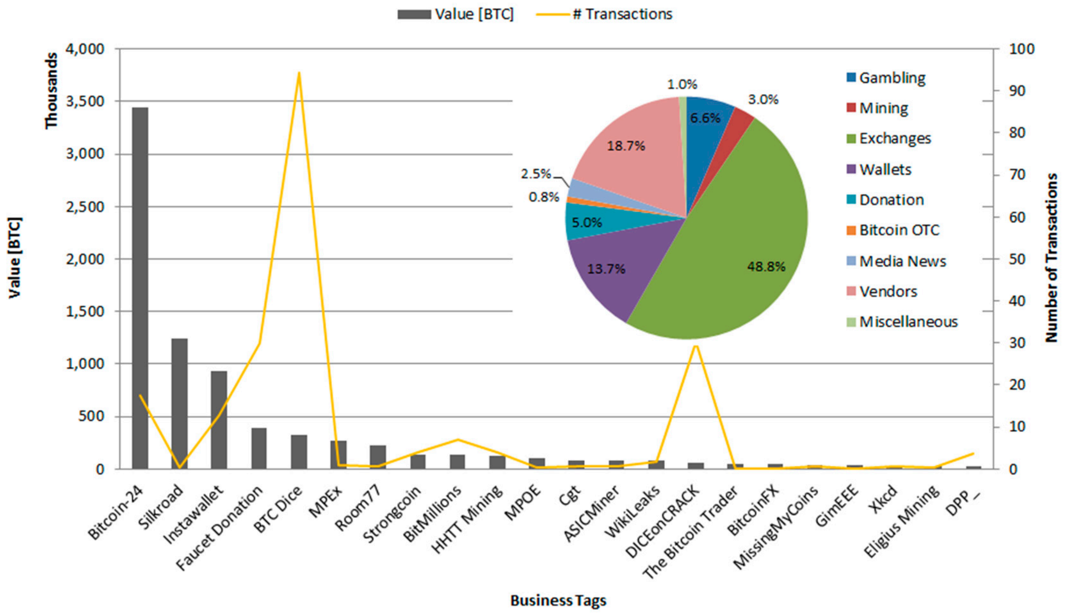


Figure 8. Top 25 Businesses (Value in BTC).

This relationship can be seen when computing the ratio of the number of executed transactions divided by their respective value (T/V ratio). Figure 9 shows the ratio, aggregated for every business category. As indicated in the top 25 statistics above, the T/V ratio for the entire dataset confirms the previous result. With a ratio of 25.4, the gambling services carry by far the smallest amount of Bitcoins per transaction; around four Bitcoins are transferred in one transaction on average. The exchanges and vendor business have the smallest ratio with 0.5 and 0.1, respectively. Hence, even on a much larger scale of classified data (~54.56%, exclude n.a.) in comparison to the top 25 businesses (~1.5%), the relationship between the number of transactions and the value stays quiet stable among the business categories.

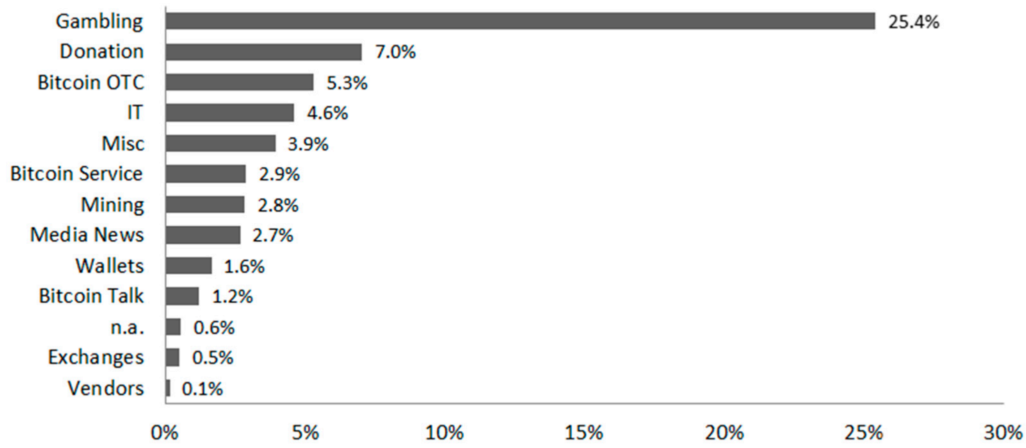


Figure 9. Transaction/Value Ratio.

To analyze the transaction value distribution more thoroughly, the transacted value in BTC is arranged in several bins from the lowest transacted value (0.00000001 BTC) to the largest transacted value (500,000 BTC). The business activity in each range is measured by the number of transactions (relationships). A transaction can incorporate several output relationships with different values; hence, the number of relationships was taken to cover the entire spectrum of transacted values. The business categories were ranked according to their portion of relationships within the range, and the top three businesses are presented in Table 4. The first eight bins, which include the transaction values from 0.00000001 to 1.0 BTC, cover around 63% of all relationships.

Table 4. Transaction Value Distribution.

Transaction Value [BTC]		#TXs	%	Top 3 Business Categories						
Low	High			1st		2nd		3rd		n.a.
0.00000001	0.00001	2,546,657	6.8	Gambling	60.0%	Media News	3.3%	Misc.	3.2%	33.5%
0.00001	0.0050	3,547,994	9.5	Gambling	43.5%	Misc.	5.7%	Media News	2.9%	47.9%
0.0050	0.0100	1,056,999	2.8	Gambling	77.4%	Exchanges	0.7%	Misc.	0.3%	21.6%
0.0100	0.0110	2,187,115	5.8	Gambling	57.0%	Mining	4.0%	Exchanges	1.2%	37.8%
0.0110	0.0199	1,928,654	5.1	Gambling	62.2%	Mining	0.8%	Donation	0.6%	36.5%
0.0199	0.0505	3,133,778	8.4	Gambling	62.5%	Mining	3.4%	Exchanges	0.8%	33.3%
0.0505	0.1001	2,387,548	6.4	Gambling	59.2%	Mining	3.8%	Exchanges	0.8%	36.2%
0.1001	1.0000	7,160,737	19.1	Gambling	55.7%	Mining	4.4%	Exchanges	1.4%	38.5%
1.0000	2.0008	2,645,839	7.1	Gambling	34.7%	Mining	5.9%	Exchanges	1.6%	57.9%
2.0008	10.000	3,632,013	9.7	Gambling	30.4%	Mining	5.1%	Exchanges	2.3%	62.2%
10.00	50.590	3,759,223	10.0	Gambling	12.7%	Mining	9.8%	Exchanges	2.8%	74.6%
50.59	100.09	703,960	1.9	Mining	11.2%	Gambling	6.1%	Exchanges	5.6%	77.1%
100.09	499.06	622,339	1.7	Exchanges	7.0%	Gambling	5.3%	Mining	4.7%	83.0%
499.06	1,000.0	197,254	0.5	Exchanges	2.8%	Gambling	1.3%	Mining	0.3%	95.6%
1,000.0	10,009	134,783	0.4	Exchanges	1.2%	Gambling	0.5%	Vendors	0.1%	98.1%
10,009	100,000	20,353	0.1	Exchanges	0.3%	Vendors	0.05%	Wallets	0.04%	99.7%
100,000	500,000	206	0.001	Exchanges	36.4%	Vendors	1.9%	-	-	61.7%

As indicated above, the gambling businesses encompass most of the transactions (relationships) in the network, but with a decreasing trend in higher value regions. In ranges with transacted values above 50 BTC, the major business switches to mining and above 100 BTC to exchanges. An interesting fact is that gambling is the second major business in the range from 50 to 10,000 BTC. The vendors appear at the very end of the range as second major business, which is not surprising when considering the large volumes traded on Silkroad. Other business categories such as gambling, mining, and exchanges are driven by SatoshiDICE, Deepbit, and Mt.Gox, respectively. One needs to be aware of the n.a. column in the table that states what percentage of transactions (relationships) within a range

are not associated to a business category. Although this table gives a good indication on how business categories are distributed within different value ranges, the numbers might change due to increased tagged services in the Bitcoin economy.

In the next statistic the composite of business categories over time are shown. Figure 10 displays the composition in terms of the number of transactions aggregated per month. For comparison reasons, the actual numbers of transactions executed per month (as sum over all business categories; but only tagged transactions, ~1.7%) are inserted as an indicator for network activity. The Bitcoin Talk users were the first business category that could be associated with transactions in April 2010. Although they make up 100% of all transactions, the network activity measured by number of transactions is very low. This group of users can be seen as the supporter of the Bitcoin economy that actively exchange information and discuss several issues regarding Bitcoins on the known forum [45]. Hence, it is not surprising that they were among the first active participants. One can see that the business category donation became more active over time. This fact can be attributed to services such as the Faucet Donation, which donate small amounts of Bitcoins to attract more users to the economy. In the time from June to December 2010 more and more businesses were attracted to the Bitcoin economy such as Media News, Bitcoin Services, Mining, provider of IT services as well as miscellaneous businesses. In the beginning of the year 2011 exchange platforms such as Mt.Gox and Bitcoin-24 entering the economy. In comparison to other business categories, the exchanges can be attributed to a rather small number of transactions over time.

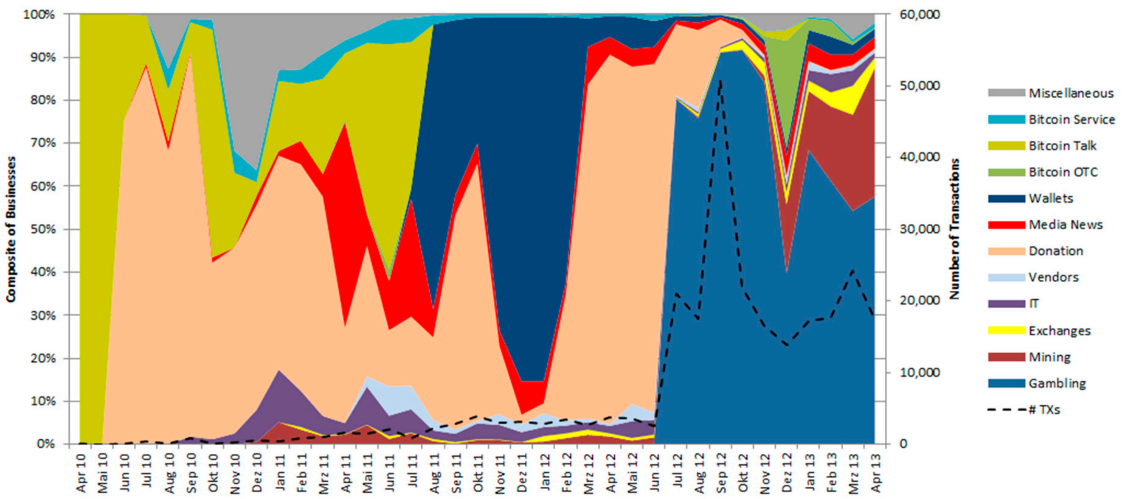


Figure 10. Composite of Businesses over Time (in Terms of Number of Transactions, #TXs).

In February 2011 the well-known vendor Silkroad started its business. The following media attention about the goods that were sold on this platform attracted more users and subsequently the network activity increased. Support of independent and liberal media and news platforms and the donation via Bitcoins made up a large portion of transactions in the first half of 2011. With the emergence of online or web wallets to hold Bitcoins, more users could then easily store and transact their Bitcoins in a convenient way; thus increasing activity and transactions related to the web wallet business. In this statistic the category is mainly driven by one of the first services called Instawallet that launches its business in April 2011. The most active time for wallet services were in the time from August 2011 to February 2012, compared to other business categories. The introduction of Bitcoin games in mid-2012, especially dice games such as SatoshiDICE and BTC Dice, resulted in an inflation of executed transactions in the Bitcoin economy. The gambling category makes up the largest portion of transactions in the network since its introduction. Between October 2012 and March 2013, the speculation on exchange rate movements surged and one can see that Bitcoin OTC trader become very active in this phase. The activity of the mining business also increased, since it is more profitable to

donate computing power in times where miners can exchange their Bitcoins at higher exchange rates into fiat currencies.

Overall, one can see a high fluctuation in the activity of different business categories. Again, these results can just be seen as an indicator because conclusions about transactions that do not have a business tag cannot be made. Comparing the results in case of the three major businesses in the Bitcoin economy gambling, exchanges, and mining with their larger representatives SatoshiDICE, Mt.Gox, and Deepbit, respectively, there is no significant correlation or even a negative correlation. Hence, the development of a business category over time is not representative for particular services related to this category.

For the complete picture the composite of business categories over time in terms of the *transacted value* in BTC is shown in Figure 11. The first thing that can easily be recognized in comparison to the previous statistic is the development of the donation business. In the early stage of the Bitcoin economy the transacted value in the network can be mainly attributed to early adopters such as Bitcoin Talk users, media news and miscellaneous services. To attract more users in the early stage, Bitcoins were donated to potential interest parties; thus, the donation business makes up around 60% of transaction volume in the time from June to September 2010. Then the attributed value decreases in comparison to other emerging businesses such as IT, media news, exchanges, and vendors. The start (April 2011) of the Silkroad vendor, which mainly drives the vendor business according to the transacted value in this statistic, incorporates large portions of the transacted Bitcoins. The tremendous increase of transacted value in the case of the Silkroad vendor is mainly explained by transactions related to the address "1DkyBEKt . . . ", which is believed to be associated with Silk Road. In the active time of this address (January–September 2012) it received large volumes of Bitcoins until August 2012; subsequently, Bitcoins were aggregated and withdrawn from this address. One can see that the suspicious address associated to the vendor Silkroad dominates the business category vendors within the network. Meiklejohn, *et al.* [8] analyzed this particular situation more thoroughly and came to a similar conclusion, although they incorporate different businesses in their vendor category. During the speculation phase, exchange platforms transact huge volumes of Bitcoins and were attributable for around 80% to 95% of transacted value. There is also a plunge of transacted value in the gambling business, while at the same time the exchange business surged. An explanation might be that users shift Bitcoins from the gambling businesses to exchange platforms in anticipation of higher rewards due to trading activities against fiat currencies.

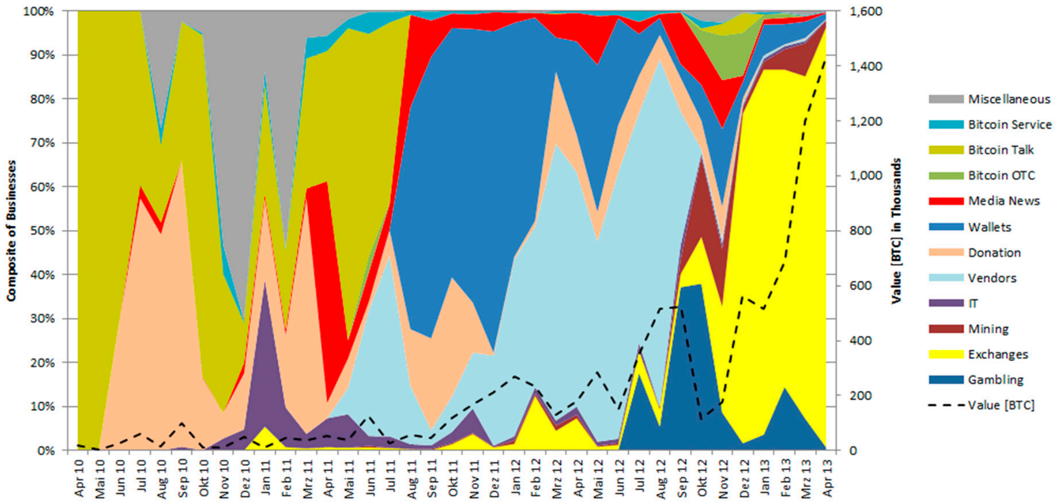


Figure 11. Composite of Businesses over Time (Value in BTC).

6.1.3. Geography of the Bitcoin Economy

Aggregations on the country and regional level are applied to get insight into the geographic distribution of the Bitcoin economy. The geo-location information is related to the IP address

that can be linked to an executed transaction in the Bitcoin network. The extracted IP addresses from Blockchain.info result in 40,329 distinct geo-locations. Transactions that are executed via the Blockchain.info node are tagged with 127.0.0.1 (*i.e.*, the non-unique localhost address), around 10.7% of all transactions. There are also transactions that could not be related to an IP address and are tagged with 0.0.0.0, around 16.6% of all transactions. The following statistics are based on the 72.4% of transactions that could be linked to an IP address. Furthermore, one has to exclude IP addresses that are associated to anonymous services such as Tor, proxy, and VPN servers. With the scraped IPs from anonymous services, around 1.6% of transactions could be linked to this kind of services.

Figure 12 shows the number of transactions and the associated value in BTC per country. One can clearly recognize that the U.S. and German market are by far the most active, followed by France, Russia, and Canada *etc.* The U.S. market alone incorporates around 38.4% of transactions and carrying around 36.7% of the Bitcoin volume in the economy.

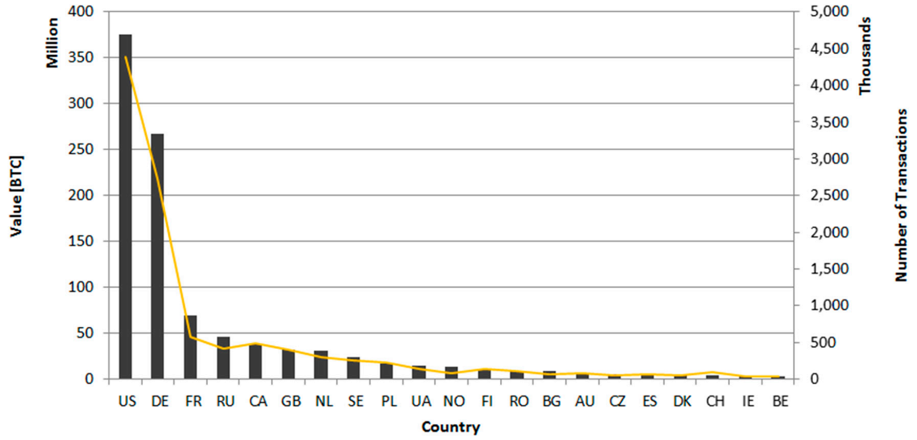


Figure 12. Number of Transactions and Value in BTC per Country.

Since there is a high correlation of 0.996 between the number of transactions and the value in BTC on the country level aggregation, the focus is on the value in BTC for measuring the activity of Bitcoin users among different countries. The first global representation of the Bitcoin network in Figure 13 shows the geo-located IP nodes that were used to execute transactions until the 10th April 2013. There is a high amount of IP nodes in Europe and the U.S. When considering areas with a higher concentration such as the east coast of China, Australia, Brazil, the southern area of Canada and Scandinavia, or western Russia, there might be a positive relationship between well-developed countries with a good infrastructure and the usage of Bitcoins.

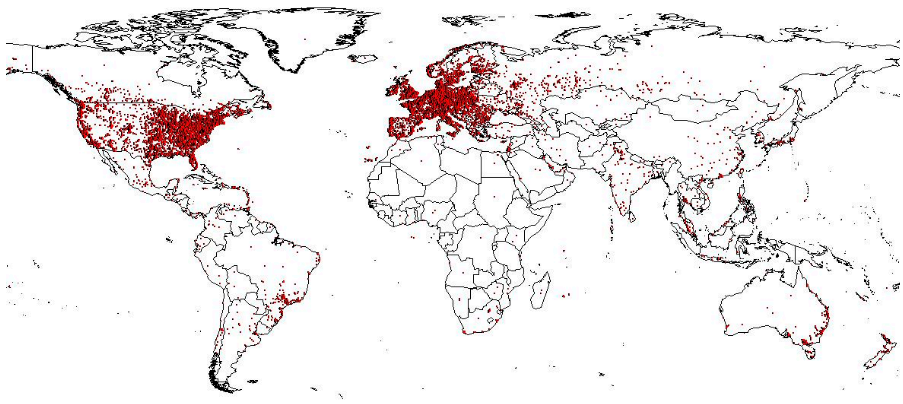


Figure 13. Global Distribution of Geo-located Internet Protocol (IP) Nodes.

Figure 14 shows the transaction volume in BTC per country on a global scale with a range from 1000 BTC to around 375 million BTC. As indicated above, well-developed countries with a good Internet infrastructure are dominant in the Bitcoin economy. Germany and the U.S. are the major markets with trading volumes of around 266 million BTC and 375 million BTC, respectively. One can also see that the emerging markets such as Russia, Brazil, or China becoming quite active in the economy.

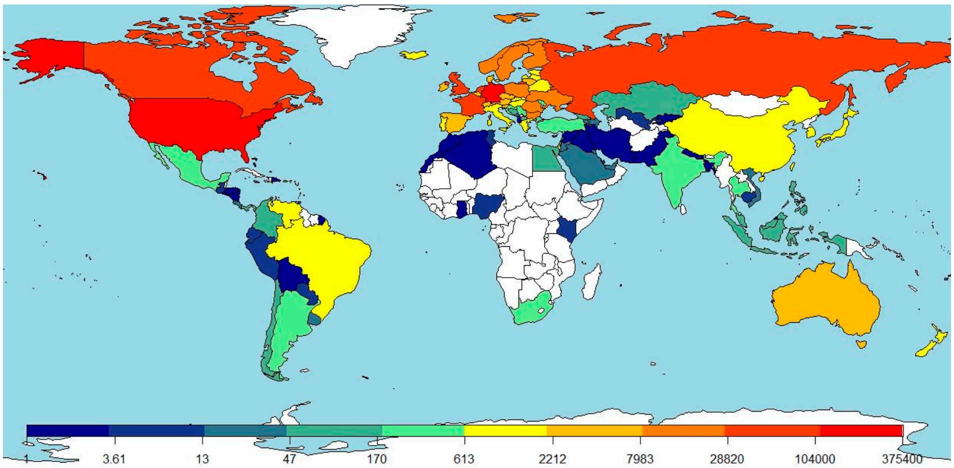


Figure 14. Transaction Volume in BTC (in Thousands) per Country.

The growth of particular countries is shown in Figure 15 as examples of network emergence in five developed markets (U.S., Germany, Australia, France, and Canada) and five growth markets (China, Russia, India, Brazil, and Thailand). There is an almost linear growth in the number of used IP nodes within the network. Interesting is the rather small number of IP nodes in countries such as Russia (480 nodes) and the respective Bitcoin volume of around 45.7 million BTC in comparison to countries such as Canada (1722 nodes) with a transacted volume of 37.5 million BTC.

Figure 15. Geographic Network Emergence over Time for Particular Countries.

The composite of particular developed countries in the Bitcoin network is measured by the transaction volume over time and depicted in Figure 16. One can see that the U.S. was the first country with transactions that could be linked to IP nodes in the network. In this early stage of the Bitcoin economy Germany and especially Australia became more active, although the overall transaction volume stays at lower levels. Since more developed countries such as Canada, France, and the Netherlands could be related to transactions in the network, the geographic contribution of these countries seems to be stable over time (February 2012–April 2013). Even the tremendous increase in

transaction volume with a peak of around 270 million BTC in September 2012 had no influence on the composite of countries in that time frame. This indicates that these countries and their respective users behave in the same way in the Bitcoin economy (*i.e.*, all countries increased their transacted volume and lowered it within that particular time frame).

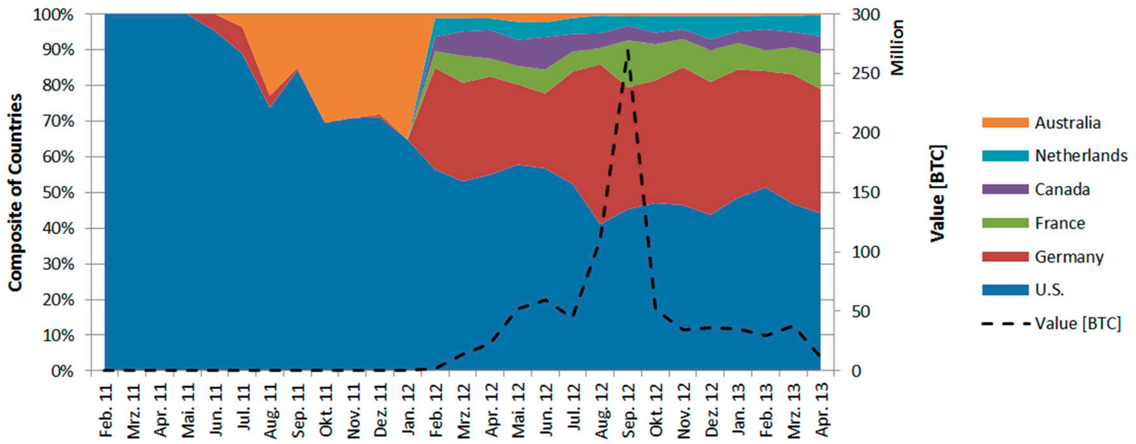


Figure 16. Composite of Developed Countries over Time (Value in BTC).

Figure 17 shows the same statistics for three emerging markets and three countries that were hit by the European financial crisis. China is the first of the emerging countries that could be linked to transactions in the network.

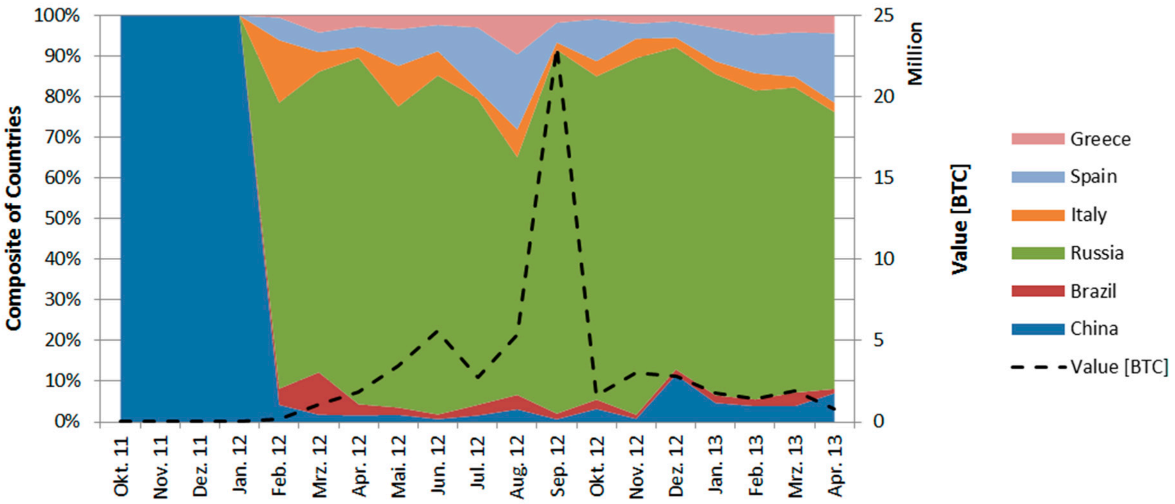


Figure 17. Composite of Emerging Countries over Time (Value in BTC).

With the linkage of transactions executed in Russia starting in January 2012, Russia becomes the major actor among emerging markets. As one could see in the previous statistics for the developed countries, the fluctuations in contribution to the Bitcoin economy are quite stable and not influenced by the transacted volume. The huge impact of the Russian market and the rather low influence from China when considering the transacted volume can be explained by the business distribution of these countries that are shown in the following statistics.

Although just a small fraction of the volume could be linked to business categories, the statistics give a good insight in the Bitcoin economy of particular countries. When looking at the European countries Germany, Sweden, and France (Figure 18), one can see that the distribution of businesses is almost the same in these countries with a focus on the mining business with around 56%. The U.S.

Bitcoin economy is different from the European since the largest transaction volume is linked to the gambling business with around 66% and just 19% can be associated to mining activities. Furthermore, the trading activities on exchanges and with vendors are higher than in developed European countries. There is a sign that the business distribution differs between continents and not just between certain countries. When considering the North America region with the U.S. and Canada, where both have a common business distribution as it can be seen for the northern European countries.

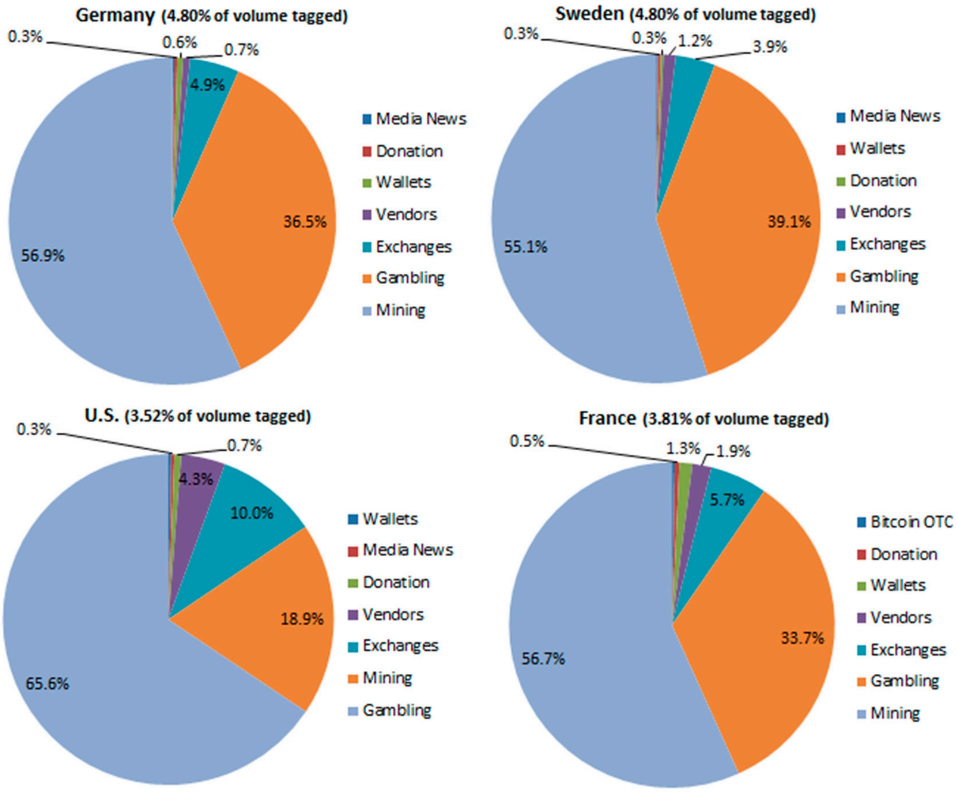


Figure 18. Transaction Volume in BTC per Business Category in Developed Countries.

The same statistics for the emerging markets (Figure 19) show much different business distributions among the countries. Russia has almost the same distribution like the northern European countries, with a focus on mining businesses with around 57%, followed by the gambling and exchanges business with around 34% and 6%, respectively. A complete different business distribution can be seen for the Chinese market with a strong focus on the gambling sector with around 87% and just a small fraction is attributed to the mining, vendors, and exchanges business. This is not uncommon since it is well known that China is one of the biggest gambling markets globally. The small contribution of transaction volume to the emerging markets volume over time shown in Figure 17 can be explained by this distribution, because gambling businesses transact very low volumes of Bitcoins compared to the mining and exchange businesses. In contrast to northern European countries, Spain has a higher share in the exchanges business with 9%. This fact can be attributed to the economic crisis in Europe and the higher interest in alternative investments as safe haven. Further investigation on the relationship between economic distressed countries and the evolvement of the Bitcoin economy in this particular countries is an interesting research topic but out of scope in this work.

The statistic in Figure 20 shows the Top 30 regions according to the transaction volume and the distribution of the three major businesses in the Bitcoin economy in this region. One can see that U.S. regions such as Texas, California, Virginia, and New York dominate the statistic. The business in the U.S. regions is mainly gambling with slight differences in the distribution for the mining and exchanges business; for example, California has a larger portion of mining businesses (21%) than

Texas (13%) and less than the New York region (32%). As indicated by the statistics on country level, Germany incorporates a large portion of the mining business, especially in Bayern (81%) and Berlin (78%). Similar results can be seen for the regions in Sweden, Netherlands, and Russia that show the same characteristic in the business distribution as on the country level. Hence, even on a smaller aggregation level the overall business distribution is stable for the three major businesses.

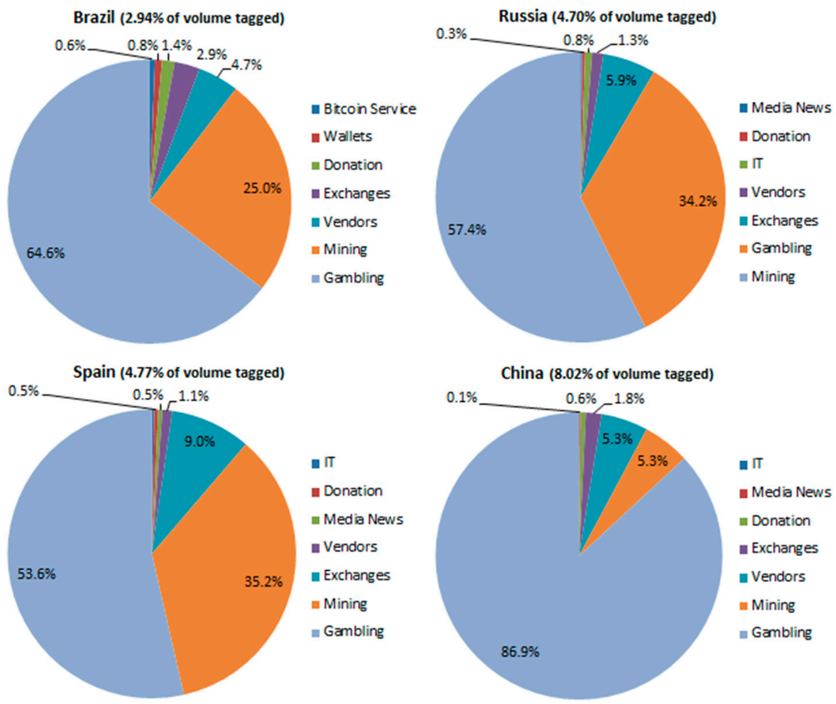


Figure 19. Transaction Volume in BTC per Business Category in Emerging Countries.

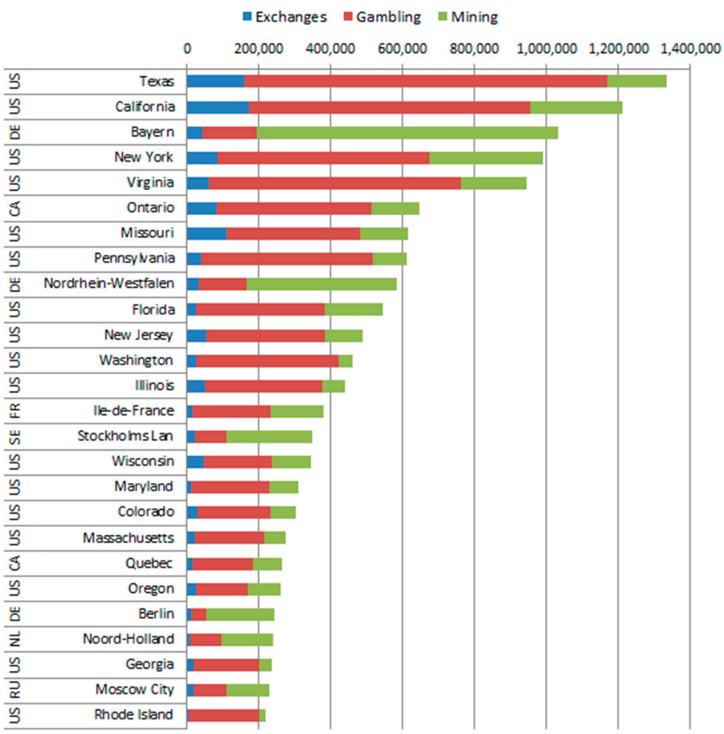


Figure 20. Transaction Volume in BTC and Business Distribution for Top 30 Regions.

6.2. Network Analysis

In the following section, network metrics will be applied for several aggregations of time, business, and country. The main objective is to investigate the structure of the Bitcoin network, identify major hubs, brokers, clusters, and find evidence for the small world phenomenon.

6.2.1. Degree Distribution and Power Law of the Bitcoin Network

The degree distribution captures the structure of the network in terms of the individual connectivity and is expected to follow a power law distribution since the Bitcoin network is considered as real world network such as the World Wide Web or social networks. To conduct the analysis within NetworkX the package "powerlaw" is required to calculate the slope coefficient a, and plot the probability density function (PDF) and complementary cumulative distribution function (CCDF) [46]. With this analysis one can examine how the power law evolves over time, differs between particular businesses or countries. A power law distribution ($P(k) \sim k^{-a}$) with a slope coefficient of $2 \leqslant a \leqslant 3$ indicates a scale-free network, which is often found in real world networks.

Figure 21 shows the development of the PDF and CCDF distribution and the associated power law fit over time. The PDF requires logarithmic binning (default in "powerlaw" package) to account for the heavy tail in the distribution and a smooth visualization. The CCDF distribution does not use binning; thus, all information of the distribution is included [46]. The plot from the Bitcoin network in 2010 shows a good fit by the power law to the PDF as well as the CCDF distribution. With increasing activity in the network in 2011 the slope α converges to a theoretically almost ideal value of 2.569, although the power law does not show a good fit for the CCDF distribution. This effect reduces over time with more user activity in the network and trade or exchange patterns. The development of the slope coefficient α for several snapshots over time is depicted in Figure 22.

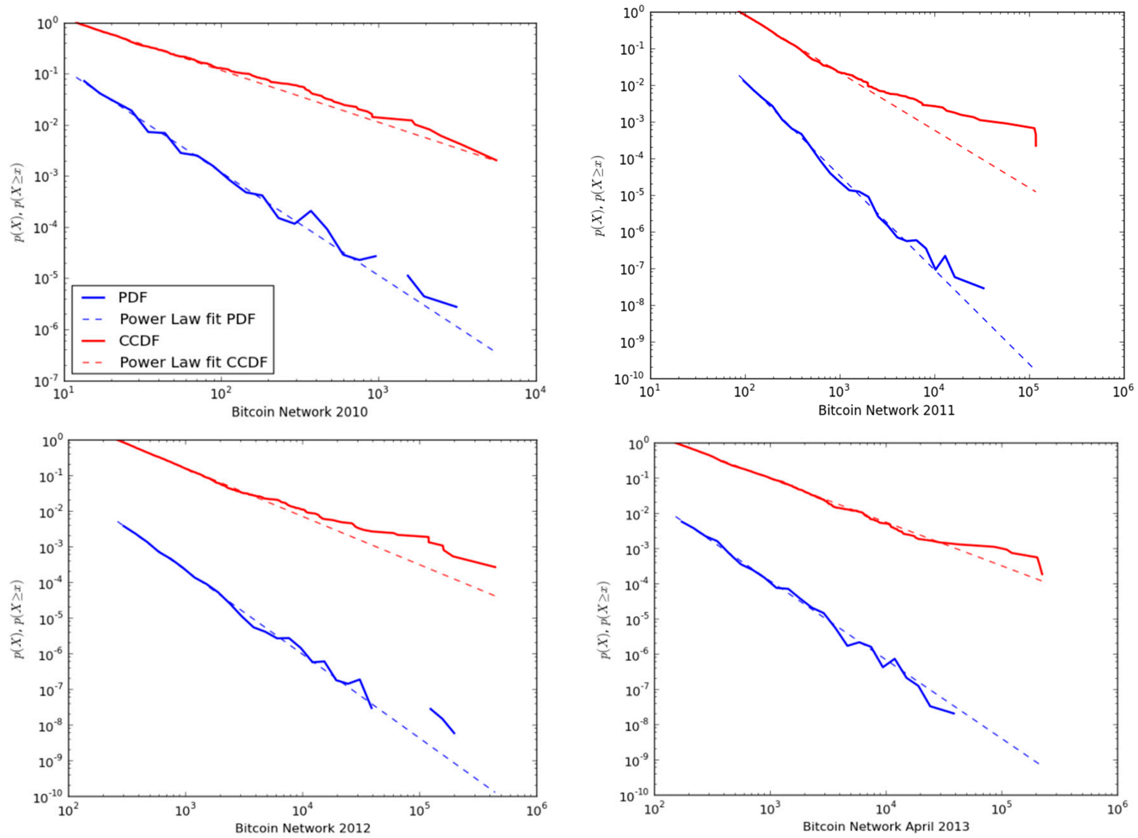


Figure 21. Degree Distribution (probability density function (PDF), complementary cumulative distribution function (CCDF)) over Time.

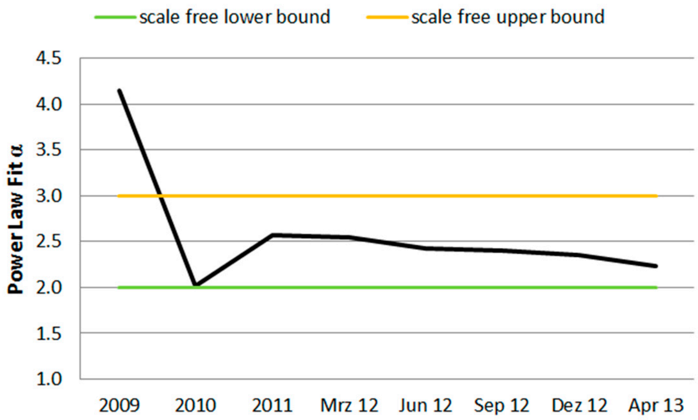


Figure 22. Development of Power Law Fit α over Time.

The same statistic for the business categories: gambling, exchanges, and mining indicate strong heavy tails when considering only particular business categories. As mentioned earlier, the categories are mainly driven by SatoshiDice (gambling), Mt.Gox (exchanges), and Deepbit (mining). These nodes have abnormal high degrees and lead therefore to the strong heavy tails. When looking at the plot (Businesses) in Figure 23 for the Bitcoin economy excluding the three major businesses one can see a good power law fit to the PDF and CCDF distribution. This might be explained by characteristics that are close to a real world economy or other social networks with various types of businesses and common behaviors by the participants. However, the slope coefficient α for different business categories in Figure 24 indicates the existence of a scale-free network for all business categories except the wallets business. Despite the strong heavy tails, the businesses exchanges and mining have a very good slope coefficient α with 2.495 and 2.517, respectively.

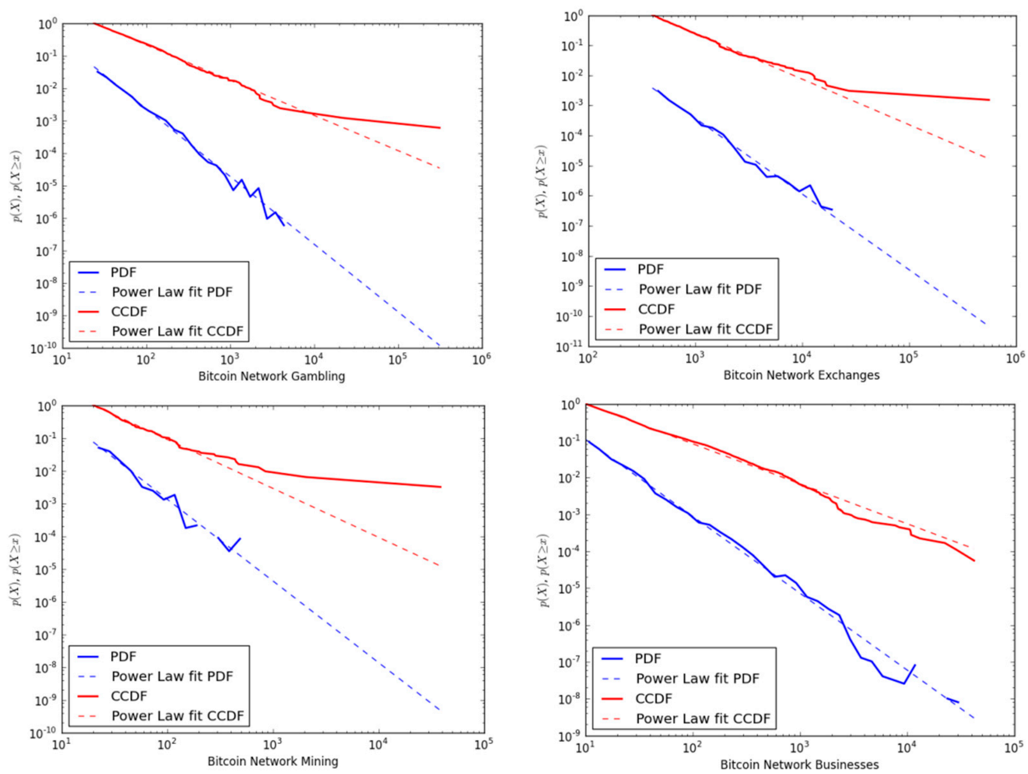


Figure 23. Degree Distribution (PDF, CCDF) for different Business Categories.

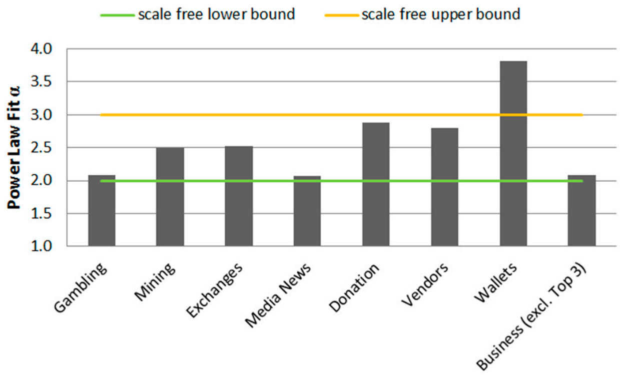


Figure 24. Power Law Fit α for Business Categories.

The degree distribution on country level aggregations reveals again the existence of a scale-free network (Figure 25). The major Bitcoin markets Germany and the U.S. show a good power law fit with a slope coefficient α of 2.132 and 2.281, respectively. The plots for Russia and Brazil, the representatives for emerging markets, illustrate that the power law does not fit the PDF and CCDF distribution as good as in the case for the developed countries. This cannot be seen as a general case, since Sweden has a similar power law fit to the degree distributions like Russia. In both countries the business distribution is dominated by the mining sector. Hence, the relationship between the degree distribution (CCDF) for the mining business and for countries such as Russia or Sweden, indicating that a dominant business category such as mining in Russia have influence on the distribution on country level. This is different from the observations that were made when considering the transaction value in different countries. In fact, the degree distribution is derived from the number of in-going and out-going transactions per node regardless of the value that is transacted.

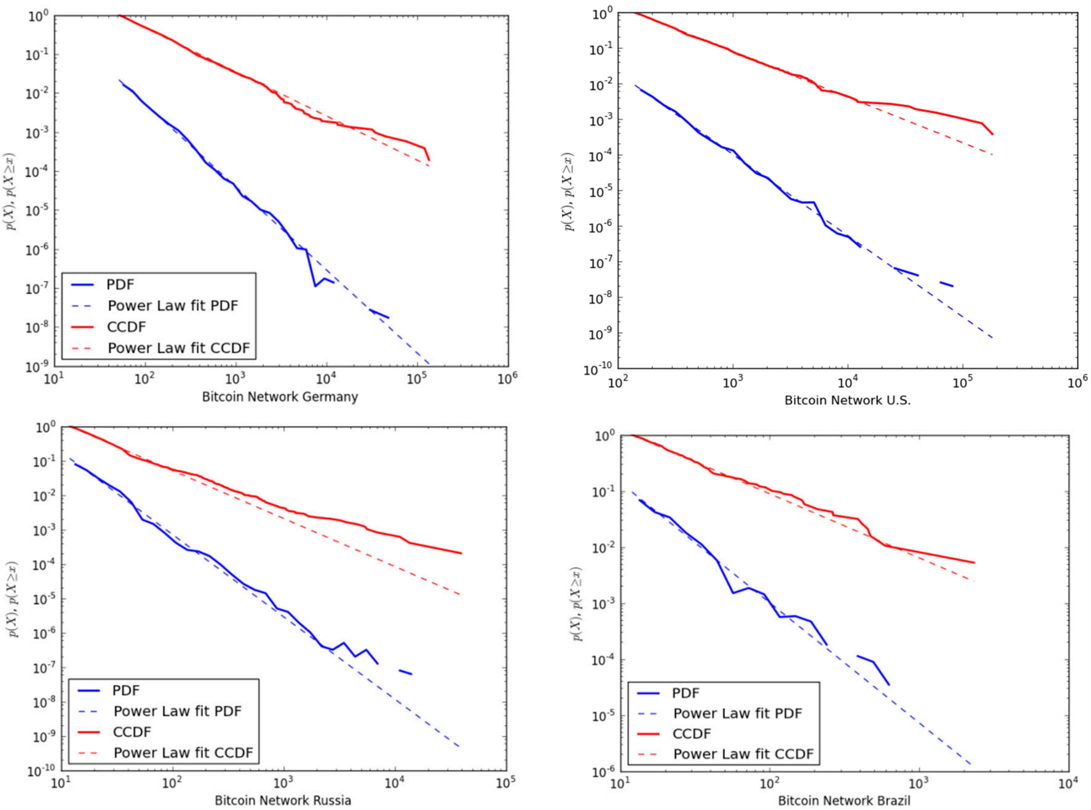


Figure 25. Degree Distribution (PDF, CCDF) for different Countries.

Figure 26 shows the power law fit for different countries. The slope coefficient α for all investigated countries is in the range that determines the existence of a scale-free network, regardless of the number of executed transactions.

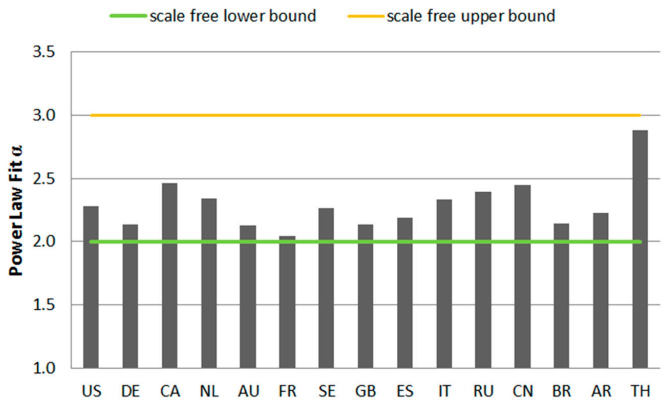


Figure 26. Power Law Fit α for Countries.

Analyzing the degree distribution (PDF and CCDF) of several aggregations on the time, businesses, and country level, reveal that the Bitcoin network follows a power law distribution, although not over the entire value range. With increasing activity (executed transactions) in the network the power law fit to the degree distribution improves. In some cases the plots show deviations between the CCDF distribution with strong heavy tails and the power law fit. The "powerlaw" package performs the calculation steps for fitting the power law automatically; hence, one cannot draw direct relationships between the power law fit to the CCDF distribution and the actual calculated power law fit α. Newman [31] states that just few real world networks follow a power law distribution over their entire range, and in particular not for smaller values of the variable being measured. In reality, therefore, the distribution must deviate from the power law form below some minimum value x-min [31]. In this analysis the calculated best minimal value for power law fit (x-min) and the standard deviation (sigma) is not published. For a more thorough investigation on power laws in the Bitcoin network, the statistics can be easily calculated with the "powerlaw" package in NetworkX.

6.2.2. Centrality in the Bitcoin Network

In the following analysis the network measure degree centrality will be applied to identify major hubs in the Bitcoin economy. The calculation of degree centrality is executed on the main connected component of the subgraphs for several aggregations to discover differences between certain businesses and countries.

The degree centrality measure for the entire Bitcoin network in the most active time from September 2012 until April 2013 is depicted in Figure 27. When considering the entire Bitcoin economy, the node 11 (Mt.Gox) can be seen as the major hub with a degree centrality of 0.094. Mt.Gox was the largest exchange platform at this time and the trading activity surged due to heavy speculations on the BTC/USD exchange rate. Furthermore, exchanges serve as entry and exit point between the real economy and the Bitcoin economy. The second major hub in the economy is the gambling business SatoshiDICE with a degree centrality of 0.075. Although it incorporates by far the most transactions in the network (~46.9%), it is not the largest hub. The node 29 is also associated to the Mt.Gox platform and has the third highest degree centrality with 0.067. Mt.Gox occurs more often because the node is not directly marked with the business tag, but the related transaction that a node has executed in the network. An increasing number of transactions marked with a business tag that was executed by a certain node indicate the control of this node by the business. Instawallet, one of the largest web wallet services, is the fourth major hub with a degree centrality of 0.043. Web wallets bundle deposits from many users and are used to store Bitcoins centrally in the web. Therefore, Instawallet become a central node from where many users execute their transactions within the Bitcoin economy.

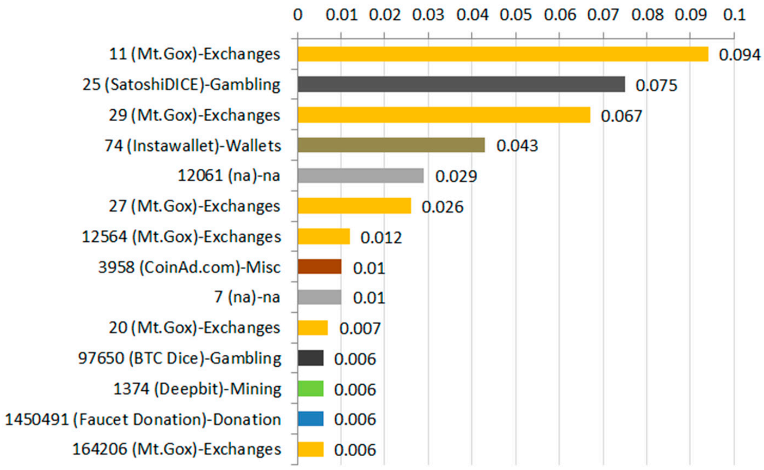


Figure 27. Degree Centrality in the Bitcoin Network (September 2012–April 2013).

The miscellaneous service CoinAd.com that spends Bitcoins for viewing or clicking certain ads is related to 674 transactions, which incorporate over 142 thousand relationships to other users. Thus, despite the low number of transactions the service is among the most central nodes within the network. Another important service, the mining pool Deepbit, has a rather low degree centrality with 0.006, although it incorporates the second highest number of transactions (~684,000) in the network. A reason might be that a majority of related transactions are not part of the main connected component graph.

The statistics in Figure 28 reveal that particular businesses make up the most central hubs within certain business categories such as gambling, exchanges, and mining. SatoshiDICE is the largest dice game operator within the Bitcoin network and has a degree centrality of 0.779. A degree centrality with the highest possible value of 1.0 would state that a business is connected to all nodes in the network. The largest exchange platform Mt.Gox is the major hub in the exchange subgraph with a degree centrality of 0.62. Compared to other business categories, the second highest degree centrality belongs to the web wallet service Instawallet with a value of 0.03. This could be explained by the fact that many Bitcoin users transact via their web wallet instead of using local clients. The major hub in the mining business is Deepbit, the largest mining pool in the network, with a degree centrality of 0.876. In case of the donation business, the first and second major hub is controlled by the Faucet Donation. Instawallet and Bitcoin Faucet are the major hubs in the wallet subgraph with a degree centrality of 0.395 and 0.223, respectively. The media and vendor business do not show dominant hubs within their respective business category.

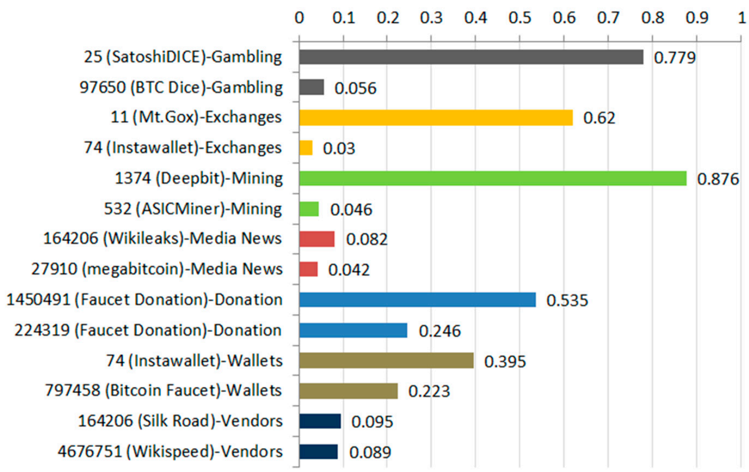


Figure 28. Degree Centrality per Business Category.

When looking at the top three major hubs in the network for different countries, one can see that the primary Bitcoin markets (U.S. and Germany) have almost the same distribution of degree centrality (Figure 29). Common facts among all considered countries are the businesses that make up the major hubs such as SatoshiDICE and Mt.Gox. The gambling business SatoshiDICE plays a very dominant role, especially in Russia and Australia, with a degree centrality of 0.149. France deviates slightly, because Instawallet is the third largest hub that indicates a higher usage of web wallet services in that country.

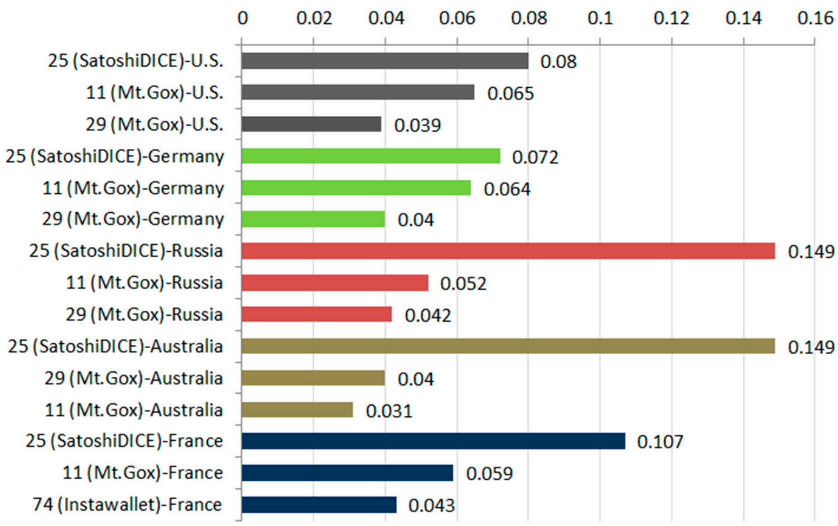


Figure 29. Degree Centrality per Country.

One can see that the three major businesses in the Bitcoin economy are also dominant on several country aggregations and within their respective business category. Hence, the economy is analyzed without these businesses to get more insight on other participants in the network (Figure 30).

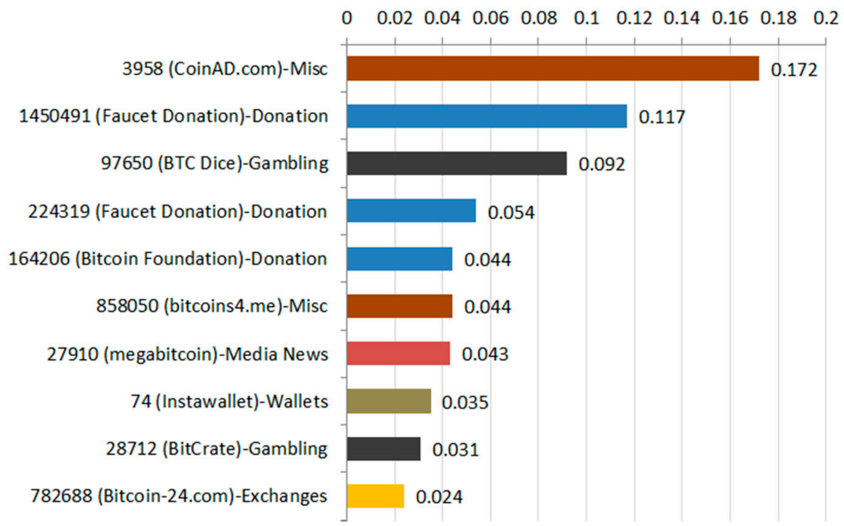


Figure 30. Degree Centrality for Business (Excluding the Top 3).

The business with the highest degree centrality (0.172) in this subgraph is CoinAd.com. As mentioned above CoinAd.com is only related to 674 transactions but incorporate over 142 thousand relationships in the network. An interesting finding is that the donation services such as Faucet Donation and Bitcoin Foundation are very dominant in comparison to the gambling business sector. Furthermore, the second

largest exchange platform Bitcoin-24.com has a low degree centrality of 0.024. Although businesses such as BTC Dice, Instawallet, or Bitcoin-24.com are related to more transactions, the actual number of relations to other nodes (measure for degree centrality) is rather low in comparison to services like CoinAd.com or Bitcoin Foundation.

More complex centrality measures such as betweenness and closeness centrality require high computation power and are therefore applied only on small subgraphs. The betweenness centrality measure is applied to identify brokers or connectors between groups of nodes within the network. With closeness centrality one can identify the most central points from where transacted Bitcoins flow most efficiently through the network.

For this particular analysis the subgraphs vendor business and wallet business were chosen. Figure 31 shows the betweenness and closeness centrality for the vendor business category. The betweenness centrality measure indicates that Silkroad and Wikispeed are the major brokers in the vendor economy. Beside the vendor businesses, the exchange platform Mt.Gox and the web wallet service Instawallet are among the major brokers in the network. Exchange platforms serve as gateways to the real economy where vendors can trade their earnings to fiat currencies and vice versa. On web wallets users can store their Bitcoins online and trade them against goods; thus serving as connection between users and the vendor businesses. The closeness centrality measure shows that these two businesses are also the most central ones in the network.

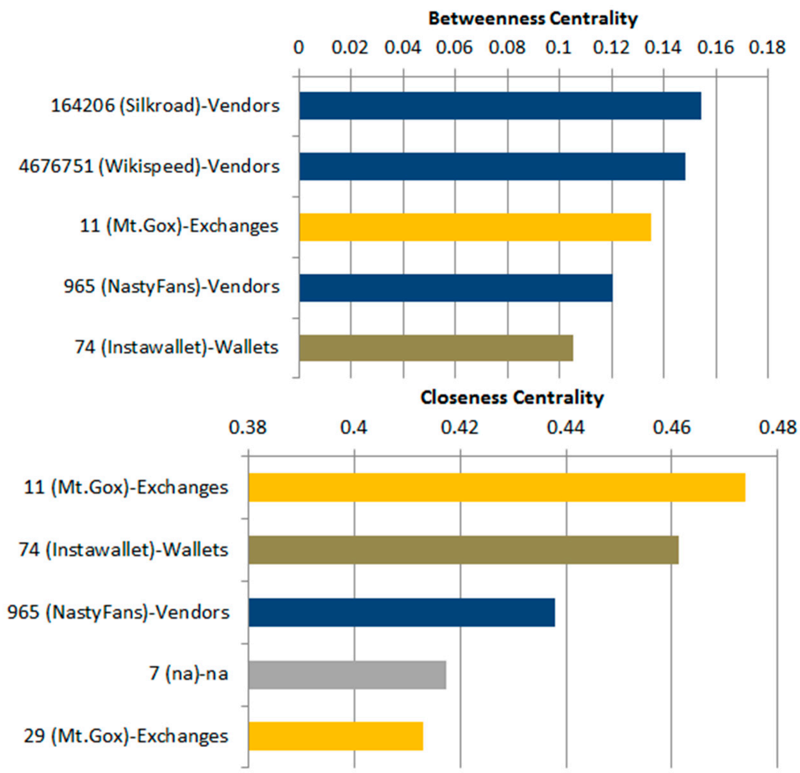


Figure 31. Betweenness and Closeness Centrality for the Vendors Business.

In terms of the wallet business (Figure 32), the major hubs Instawallet and Bitcoin Faucet are also the main brokers in the network. Interestingly, the top five betweenness centrality values belong all to wallet businesses indicating that web wallets serve as connectors between other businesses. When considering the closeness centrality, Instawallet is again the most central node in the network followed by the exchange platform Mt.Gox. Exchange platforms like Mt.Gox are very centrally positioned in the network and play an important role within the Bitcoin economy.

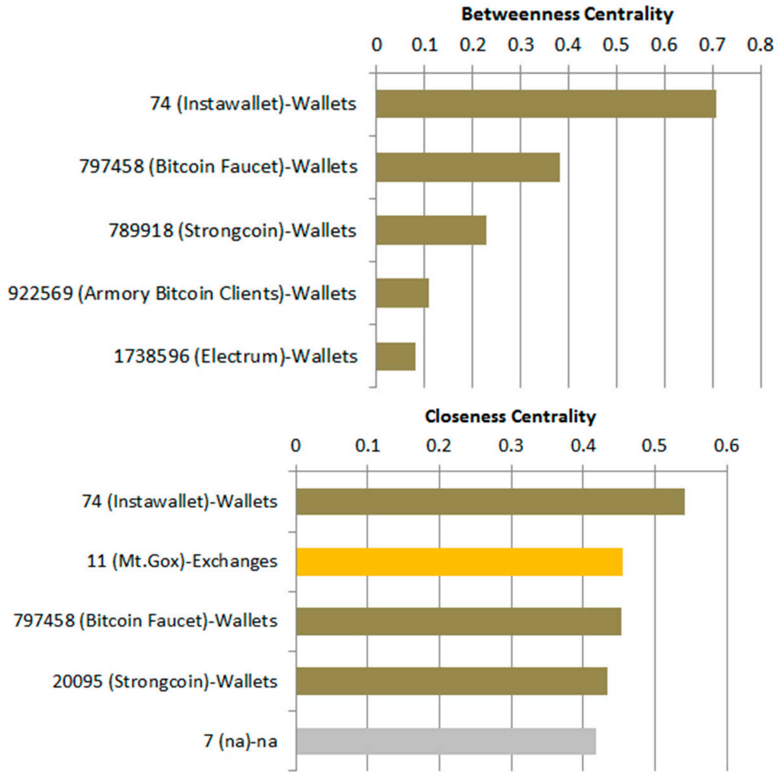


Figure 32. Betweenness and Closeness Centrality for the Wallets Business.

6.2.3. Clustering in the Bitcoin Network

In this section, the network measure average clustering coefficient is going to be applied on the time, business, and country level to investigate the global cliquishness in the graph. Furthermore, it serves as a first indicator of the small world phenomenon within the Bitcoin network. Analyzing the existence of small world networks requires high computation power and is therefore conducted on minor subgraphs on the country and business level.

When considering the average clustering measure over time in Figure 33, one can see rather high coefficients in comparison to random networks, indicating a small world network. The measure was computed on a monthly basis for the years 2012 and 2013. For the year 2011 the calculation was done quarterly. The years 2009 and 2010 were omitted from the analysis due to very low activity in the network and lots of transactions between same entities.

The average clustering coefficient decreases with increasing activity in the network. In quarter two and three of 2011 the lowest coefficients were computed, while the user activity surged in that time period. The same effect can be noted for August 2012 and March 2013. Hence, more user activity in the network reduces the global cliquishness in the Bitcoin economy.

The average clustering coefficients for different business categories are depicted in Figure 34. Because of limited computation power, the coefficients for the gambling and exchange business were calculated on subgraphs (January–April 2013). The gambling business has the highest average clustering coefficient with around 0.5. This indicates that the gambling business is tightly connected and has a high density of nodes. In contrast, the computed coefficients for other businesses are rather low but indicate the existence of the small world phenomenon. The mining business has a low average clustering coefficient with 0.012, indicating a rather separated engagement of the miners in the network.

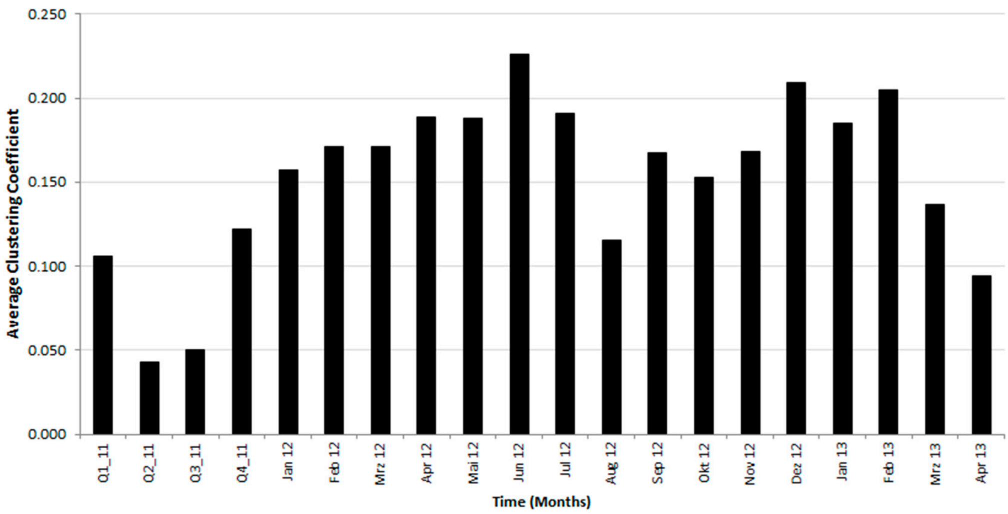


Figure 33. Average Clustering Coefficient over Time.

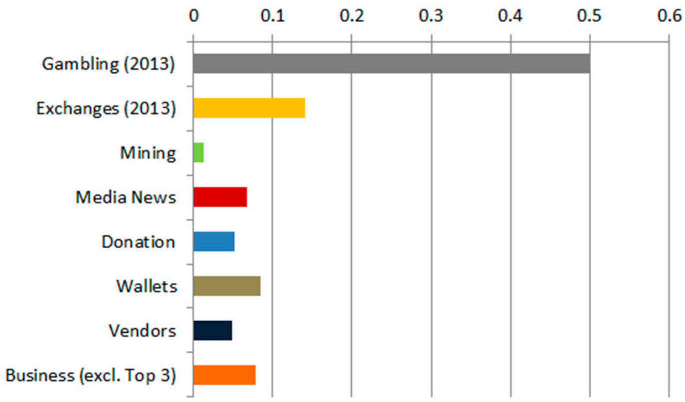


Figure 34. Average Clustering Coefficient for Business Categories.

Figure 35 shows the average clustering coefficient for selected countries. The coefficients for the major markets U.S. and Germany were calculated on subgraphs (January–April 2013). China and the U.S. have the highest avg. clustering coefficient with 0.116 and 0.130, respectively. These are also Bitcoin markets that are mainly driven by the gambling business, which has a very high average clustering coefficient. The coefficients for the other Bitcoin markets are in the range from around 0.05 to 0.08, indicating the existence of the small world phenomenon when considering the average clustering coefficient for random networks.

In the following, the hypothesis of the small world character will be tested on two business categories and four countries as representatives for these aggregation levels. To determine the existence of a small world graph one has to calculate the average clustering coefficient and the average shortest path length of the graph in question. In addition, a random graph with the same number of nodes and edges needs to be generated. When comparing the computed network measures the average clustering coefficient of the Bitcoin network has to be significantly higher than the one of the random network ($\overline{C}_{Bitcoin} \gg \overline{C}_{Random}$) while the average shortest path length has to be rather low and is approximately the same ($ASPL_{Bitcoin} \cong ASPL_{Random}$). The calculation of the average shortest path length requires high computation power for large-scale graphs and subgraphs as it is the case with the Bitcoin network. Hence, testing for the small world phenomenon is done on minor subgraphs on the country and business level.

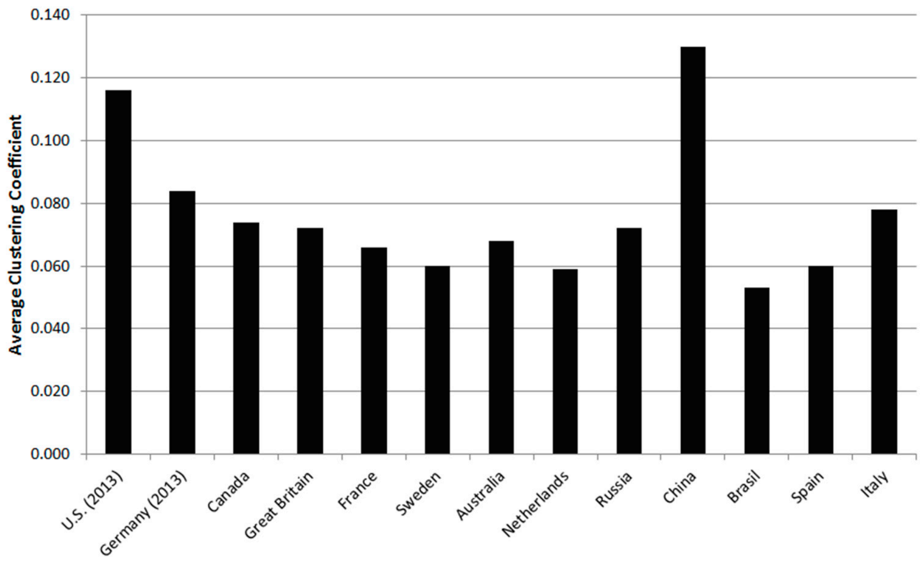


Figure 35. Average Clustering Coefficient per Country.

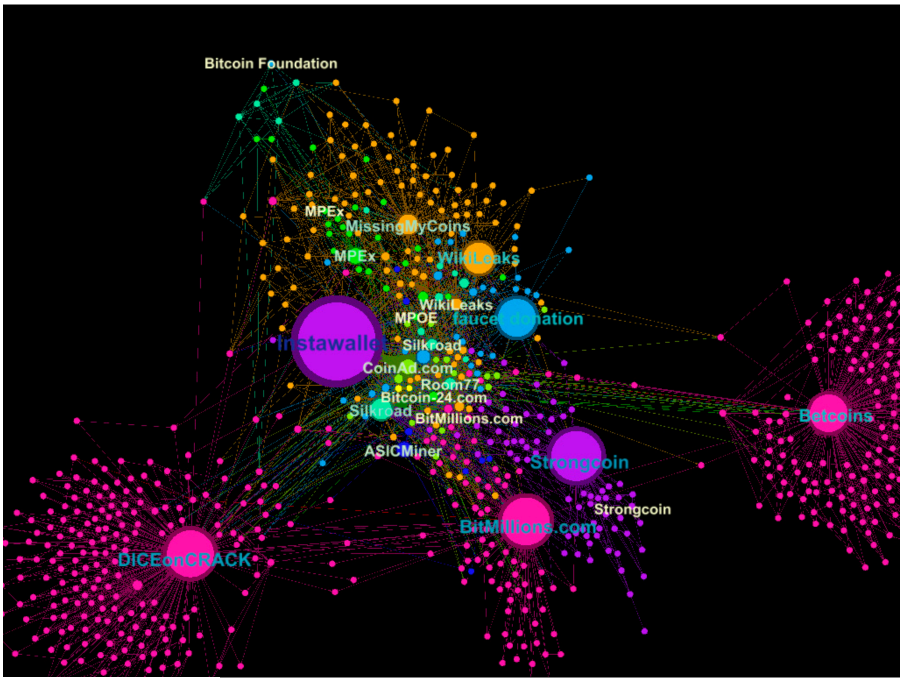
Table 5 shows the results of the small world analysis. On the country level the existence of the small world phenomenon could be approved for all considered countries. One can see that the avg. clustering coefficient is significantly higher in comparison to the random graph of the same size and that the avg. shortest path is in the same range. In case of the considered business categories, the small world phenomenon could only be approved for the wallets business while the vendors business missed the criteria mentioned above. This shows that a rather high average. high clustering coefficient alone cannot be used to determine the existence of the small world phenomenon. It serves just as a first indicator that requires further analysis on the graph and the comparison of the network measures with a random graph of the same size.

Table 5. Results of Investigating the Small World Phenomenon on Subgraphs.

Aggregates	Bitcoin Graph		Random Graph	
	AVG Clustering	AVG Shortest Path	AVG Clustering	AVG Shortest Path
Country				
China	0.130	5.15	0.00071	4.45
Brasil	0.053	4.74	0.00115	4.45
Italy	0.078	4.39	0.00091	4.23
Argentina	0.078	4.78	0.00190	4.25
Business				
Wallets	0.085	3.90	0.00402	3.10
Vendors	0.048	3.32	0.062	1.95

6.2.4. Visual Analysis of the Bitcoin Network

In the final part of the network analysis, the tool Gephi is applied to conduct a visual analysis of the Bitcoin network. The subgraph that is used is based on the tagged businesses excluding the top three businesses (SatoshiDICE, Mt.Gox, and Deepbit). Furthermore, only a certain amount of businesses were chosen that play an important role according to their number of transactions or the transaction value due to limits in computation power. The first visualization (Figure 36) shows the degree centrality per node given by the size of the node. In addition, the label tags are colored and sized by the degree centrality (large and dark blue labels are associated to a high degree and vice versa for the small degree). The nodes are colored according to their category.



Gambling	*(65.64%)*	*Gambling*: DICEonCRACK, Betcoins, BitMillions.com
Media News	*(13%)*	*Media News*: WikiLeaks, MissingMyCoins, megabitcoin
Wallets	*(9.01%)*	*Wallets*: Instawallet, Strongcoin
Donation	*(3.99%)*	*Donation*: Faucet Donation, Bitcoin Foundation
Exchanges	*(3.35%)*	*Exchanges*: Bitcoin-24.com, MPEx, MPOE
Misc	*(1.93%)*	*Misc*: CoinAd.com, bitcoins4.me
Vendors	*(1.8%)*	*Vendors*: Silkroad, room77
Mining	*(1.03%)*	*Mining*: HHTT Fund Pool, ASICMiner
Bitcoin OTC	*(0.26%)*	*Bitcoin* OTC: DPP_

Figure 36. Visualization of Degree Centrality for Important Subgraph.

When looking at the nodes in the network, one can see that they form groups of clusters for certain businesses, especially in case of the gambling business (DICEonCRACK, Betcoins, and BitMillion.com). This confirms the high coefficient from the previous clustering analysis. The highest degree centrality in this subgraph can be related to the web wallet business (Instawallet and Strongcoin), the gambling businesses, and the donation business (Faucet Donation).

Figure 37 shows the visualization of the clustering coefficients per node in the Bitcoin network. Interestingly, the nodes with a high degree centrality have a very small clustering coefficient, but the nodes around show rather high values, especially in case of the gambling businesses. The highest clustering coefficients can be seen for the exchange platform MPEx and for the nodes around the gambling businesses. In contrast, the values for the mining business (dark blue nodes) are among the lowest in the network. This again confirms the previous analysis on clustering in the Bitcoin economy, even on a much smaller scale.

Figure 38 shows the aggregated transaction volume per node. Two nodes that are associated to the vendor Silkroad have the highest value in this particular subgraph. Other nodes that transact higher volumes of Bitcoins belong to the exchange business (Bitcoin-24.com, MPEx) and the wallet business (Instawallet). In contrast, the gambling, donation, and media/news business transact rather low values of Bitcoins in the network. This confirms previous descriptive statistics on the business aggregates.

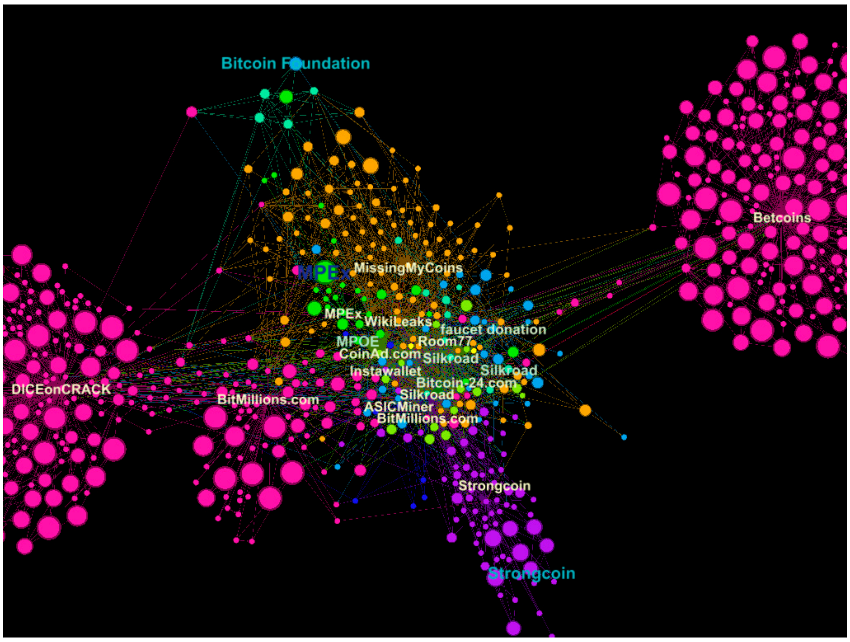


Figure 37. Visualization of the Clustering Coefficient in the Bitcoin Network.

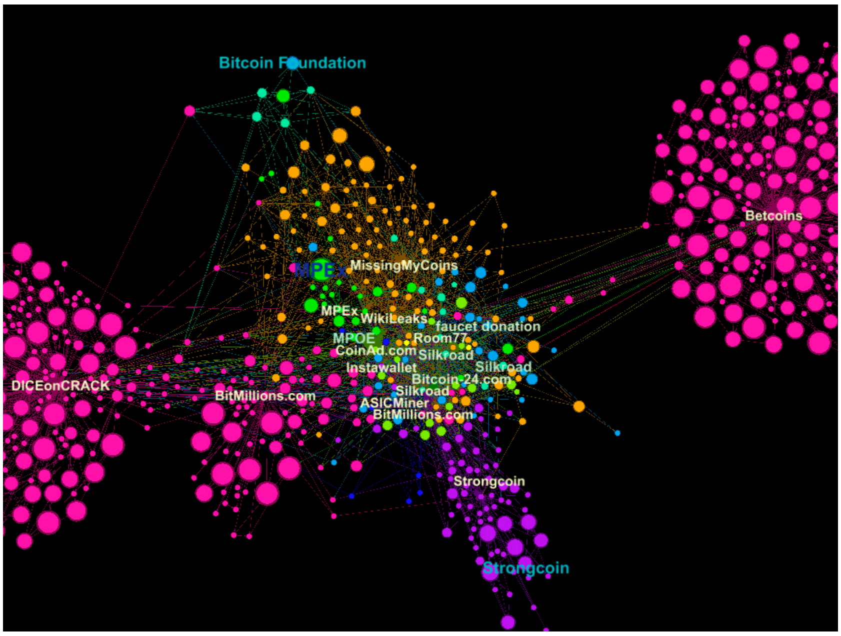


Figure 38. Visualization of the Transaction Value in the Bitcoin Network.

Another interesting node attribute, the node size, is visualized in Figure 39. The node size is determined by the number of public keys that belong to a user or economic entity and can be seen as clusters of public keys. The vendor Silkroad incorporates nearly 210 thousand public keys, while the web wallet service Instawallet and the gambling business BitMillions.com have around 110 thousand associated public keys. Goods traded on Silkroad are often related to prohibited items such as weapons or drugs; hence, anonymity is essential for the participants. The execution of transactions via several thousand public keys and the usage of newly generated public keys for every new transaction might increase anonymity. In case of Instawallet, one can assume that most of the public keys belong to different users, which use the convenient way of storing and using Bitcoins via

web wallets in the network. Thus, a large amount of public keys can be interpreted in different ways, depending on the business or service offered.

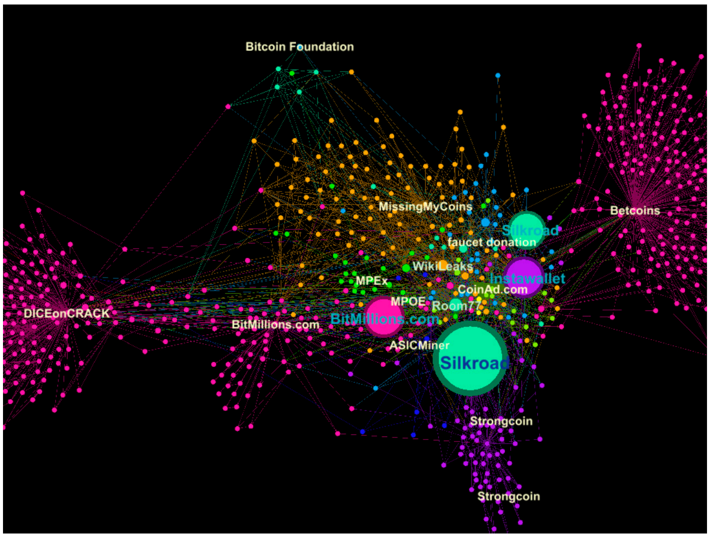


Figure 39. Visualization of Node Size (Number of Public Keys) in the Bitcoin Network.

Figure 40 shows visualizations of the betweenness per node in the Bitcoin network. The betweenness centrality highlights the brokers in this subgraph. The gambling service Betcoins has the highest betweenness centrality (0.439) in the network and can be seen as the main broker. Other important nodes that serve as central connection hubs can be related to the gambling services DICEonCRACK (0.301) and BitMillions.com (0.339) and the web wallet service Instawallet (0.163).

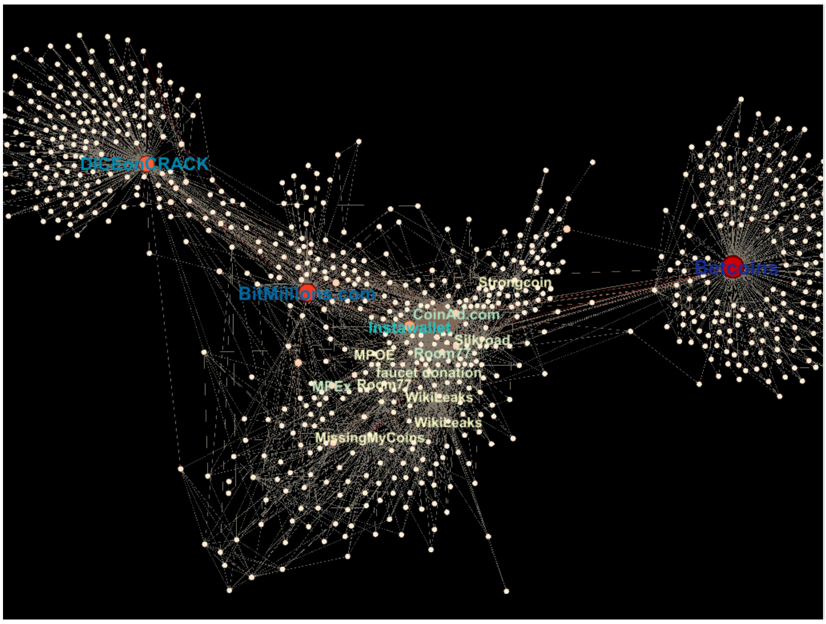


Figure 40. Betweenness Centrality in the Bitcoin Network.

The visualization of closeness centrality (Figure 41) shows the most central nodes in the subgraph from where Bitcoins are transacted efficiently. One can see that a large portion of the nodes related to the wallet business Strongcoin have the highest closeness centrality. The well-known media/news site

WikiLeaks, the vendor Silkroad, and the donation service Bitcoin Foundation are also very central in the network.

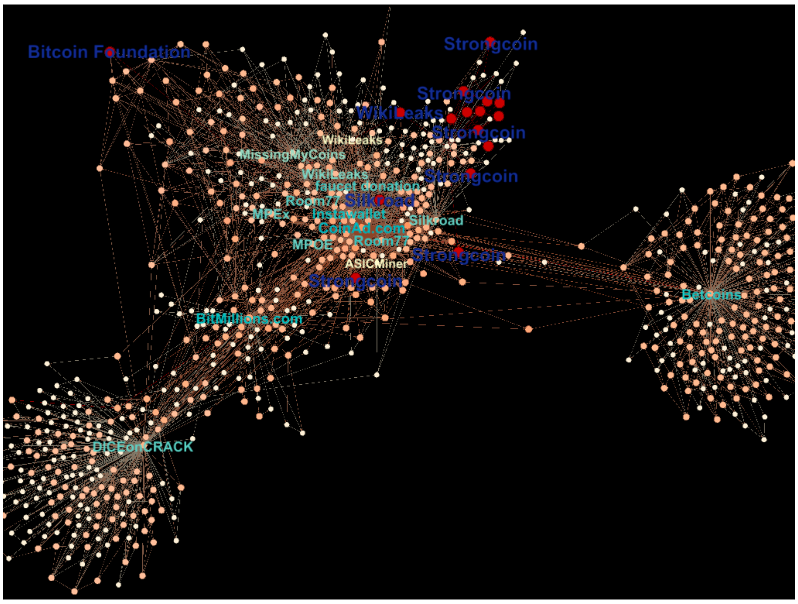


Figure 41. Closeness Centrality in the Bitcoin Network.

The final visualization in Figure 42 shows the Bitcoin network with geo-located nodes. Nodes are colored by country (and edges by the source node). For this analysis, only nodes that transact via one IP address can be considered; thus, this subgraph (tagged as Business, excluding SatoshiDICE, Mt.Gox, and Deepbit) of the Bitcoin network is smaller than in the previous analyses. Through the usage of web wallets and other central services a node might have several IP addresses and subsequently different geo-locations. In contrast, many different nodes can transact Bitcoins via one IP address, because of regional concentrations of Bitcoin users.

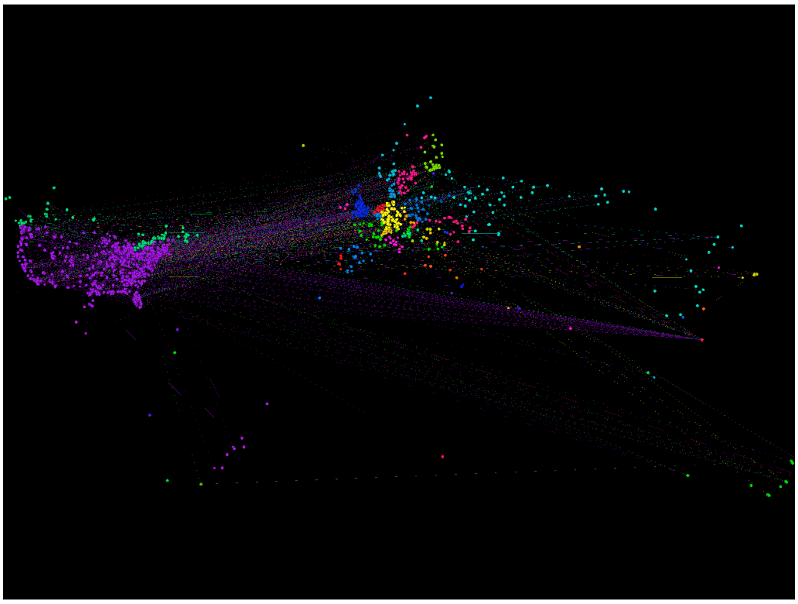


Figure 42. Bitcoin Network and Earth Geography

7. Conclusion, Limitations and Outlook

This explorative research examined the Bitcoin economy and network by introducing an enriched data. The data model incorporates the Bitcoin user network introduced by Reid and Harrigan [2] and scraped information from several websites to construct new aggregates on the business and geographical level. This information contains business tags, IP addresses, and geo-locations that could also be associated to Bitcoin users. Furthermore, trade data on the BTC/USD exchange rate and data on anonymous services such as Tor were extracted.

To conduct analysis on the business aggregation level the tags related to a transaction were categorized into 13 categories. Over 54% of all transactions could be classified. The first analysis on business categories reveals that around 48% of all transactions are related to gambling services and almost 46% are associated to the dice game SatoshiDICE. The second and third largest business according to the number of transactions is the mining pool Deepbit with 4.3% and the exchange platform Mt.Gox with 1.7%, respectively. When analyzing the number of transactions and the transaction volume for particular businesses, a different transaction pattern was found among the categories. Businesses such as exchanges, vendors, or wallets transact rather large amounts of Bitcoins, while businesses such as gambling or donation transact very small amounts of Bitcoins in the network. This was expressed by the T/V ratio (transaction to value ratio). For instance, the T/V ratio for gambling is 25 and that of the vendor business is 0.1. Further analysis on the transaction value distribution reveals that 63% of all transactions are in the range from 0.00000001 until 1.0 BTC and the gambling businesses incorporate most of them but with a decreasing trend in higher value regions. In the ranges above 100 BTC, most transactions are related to the exchange business. The development of the business categories over time shows that Bitcoin Talk users and the donation services were among the most active participants because of their importance during the startup phase of Bitcoin. Later on, web wallets, media and news, and exchange platforms enter the Bitcoin economy. With the introduction of gambling services the number of transactions gets inflated, especially by the most popular SatoshiDICE game. The differences between the number of transactions and the transaction volume for particular categories could be also observed over time.

The analysis on the geographic aggregation level was not done before on this scale and requires the exclusion of IP addresses that could be associated to Tor, Proxy or VPN services (~1.6% of transactions). When analyzing the Bitcoin economy geographically, one can see that the major markets are in the U.S. and Germany. The geographic distribution of the transaction volume reveals that Bitcoins are mainly used in countries with a good infrastructure during the analyzed time interval.

With the linkage of geo-locations to transactions with business tags, an innovative analysis of the distributions of businesses per country could be conducted. Northern European countries like Germany, Sweden, Russia, or France have a similar business distribution with a strong focus on mining with around 56%. In contrast, the U.S., Canada, and Brazil, which share a common business distribution with a focus on the gambling business with around 65%. A special case could be seen for the Chinese Bitcoin market, where 87% of transaction volume is linked to the gambling business. Another finding is that countries such as Spain, U.S., Canada, and Argentina were more engaged in the exchange business with around 10%, indicating a higher speculative behavior. In the cases of Spain and Argentina this could be related to economic and financial distress, and the searching for new save havens, while in the U.S. and Canada users are more market oriented and seeking for high abnormal returns through speculation on the Bitcoin exchange rate.

Investigation of the degree distribution and power law over time reveals that the Bitcoin network follows a power law distribution over large parts of the value range. Since 2010, the Bitcoin network can be considered as a scale-free network with a power law slope coefficient α in the range between 2.0 and 2.6 in the time horizon from 2010 to 2013. The degree distributions for particular businesses show strong heavy tails for the gambling, mining, and exchange business. These business categories are mainly driven by one business with an abnormal high degree. The power law slope coefficient α for all business categories (except the wallets business) is in the range between two and three,

indicating a scale-free network. On the country level, the degree distributions show a similar result. All considered countries have a power law slope coefficient α between two and three, indicating the existence of a scale-free network. The analysis reveals that the majority of the investigated subgraphs of the Bitcoin network are scale-free networks.

To identify major hubs in the Bitcoin network, the degree centrality was analyzed. The results on the entire Bitcoin network in the most active time from September 2012 to April 2013 reveal that the major hub nodes are controlled by the exchange platform Mt.Gox, the gambling service SatoshiDICE, and the web wallet service Instawallet. Next, the degree centrality was analyzed on the business aggregates. The results show that the dominant services in a business category are also the major hubs in the network. This is especially the case for SatoshiDICE in the gambling business, Mt.Gox in the exchange business, Deepbit in the mining business, and Instawallet in the wallet business category.

The analysis of the average clustering coefficient indicates the existence of the small world phenomenon in the Bitcoin network over time as well as on the country and business aggregation level. This kind of analysis needs high computation power and was therefore tested on minor subgraphs on the business and country aggregation level. The existence of the small world phenomenon could be demonstrated for the country aggregations China, Brazil, Italy, and Argentina. For the business aggregations, the wallet and vendor businesses were investigated. Only the wallet business could be considered as small world network. The vendor business missed the requirements. This shows that a rather high clustering coefficient is just a first indicator and needs further investigation.

Further network statistics could be applied on a representative subgraph of the Bitcoin economy to identify clusters, hubs, brokers, and most central nodes in the network. Furthermore, particular Bitcoin nodes and their interaction in the network could be identified and a geographic visualization of the subgraph was realized. This gives new insights on the Bitcoin economy in a visual way.

Several interesting aspects of the Bitcoin economy could be covered in this work, but there are some limitations that could be addressed in future research. Extensions of this work should contain most recent data of the Bitcoin network to get insight on new developments in the economy, such as the attack on Mt.Gox with the subsequent closing of the exchange platform, or the closing of the vendor Silkroad. Furthermore, the intense fluctuations of the BTC/USD exchange rate in late 2013, resulting in a record high over $1,200 per Bitcoin, could be investigated. Another method would be time series analysis on economic distressed countries such as Spain, Cyprus, or Argentina and investigations on how the Bitcoin economy evolved during this time. One could also analyze the economic development in certain countries with appropriate economic measures and regress it against Bitcoin variables. Although events that explain the movements have been presented in this work, one could link these to network analysis and also visually investigate the Bitcoin transaction flows.

Even though 54% of all transactions could be related to a business tag and category, only 1.5% of them are not associated to the major businesses SatoshiDICE, Mt.Gox, or Deepbit. Re-identification techniques introduced by Meiklejohn *et al.* [8] could be applied in addition to the Blockchain.info web scraper to link further businesses to transactions, especially for high volume transactions. With their approach and modified clustering algorithms Meiklejohn *et al.* could tag around 2200 out of 3.38 million user nodes in the network. The more conservative and reliable clustering algorithm applied in this study is based on the research by Reid and Harrigan [2] and resulted in around 6.3 million user nodes.

With sufficient computation power, future research could have a stronger focus on the network analysis of the Bitcoin economy. Then, complex network measures such as betweenness and closeness centrality, the average shortest path length, average clustering, and simulation of random networks can be applied on a much larger scale. Hence, the small world phenomenon could be investigated on large subgraphs or even on the entire Bitcoin network. Furthermore, the visualization of the Bitcoin economy could be extended on time, country, and business aggregation levels. Overall, our methods and data provide a starting point into a variety of fields for further research on Bitcoin.

Acknowledgments: The authors would like to thank Annika Baumann for helpful discussions during early stages of this research.

Author Contributions: Matthias Lischke and Benjamin Fabian jointly designed the research concept. Matthias Lischke gathered the data and conducted the analyses. Both authors jointly wrote the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: http://bitcoin.org/bitcoin.pdf (accessed on 1 March 2016).
2. Reid, F.; Harrigan, M. An Analysis of Anonymity in the Bitcoin System. In *Security and Privacy in Social Networks*; Springer: New York, NY, USA, 2012; pp. 197–223.
3. The Economist: Bitcoins. Available online: http://www.economist.com/topics/bitcoins (accessed on 1 March 2016).
4. Baumann, A.; Fabian, B.; Lischke, M. Exploring the Bitcoin Network. In Proceedings of the 10th International Conference on Web Information Systems and Technologies (WEBIST); WEBIST: Barcelona, Spain, 2014.
5. Drainville, D. An Analysis of the Bitcoin Electronic Cash System. 2012. Available online: http://cryptolibrary.org/handle/21/601 (accessed on 1 March 2016).
6. Ober, M.; Katzenbeisser, S.; Hamacher, K. Structure and Anonymity of the Bitcoin Transaction Graph. *Future Internet* **2013**, *5*, 237–250. [CrossRef]
7. Bitcoinmining: Bitcoin Mining Pools. Available online: https://www.bitcoinmining.com/bitcoin-mining-pools/ (accessed on 1 March 2016).
8. Meiklejohn, S.; Pomarole, M.; Jordan, G.; Levchenko, K.; McCoy, D.; Voelker, G.M.; Savage, S. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In *Proceedings of the 2013 Internet Measurement Conference*; ACM: New York, NY, USA, 2013; pp. 127–140.
9. Spagnuolo, M. BitIodine: Extracting Intelligence from the Bitcoin Network. Thesis, Politecnico di Milano, 2013. Available online: http://miki.it/pdf/thesis.pdf (accessed on 1 March 2016).
10. Androulaki, E.; Karame, G.O.; Roeschlin, M.; Scherer, T.; Capkun, S. Evaluating User Privacy in Bitcoin. In *Financial Cryptography and Data Security*; Lecture Notes in Computer Science; Springer: Berlin, Geramny; Heidelberg, Germany, 2013; Volume 7859, pp. 34–51.
11. Kaminsky, D. Black Ops of TCP/IP, Presentation, Black Hat & Chaos Communication Camp 2011. Available online: http://de.slideshare.net/dakami/black-ops-of-tcpip-2011-black-hat-usa-2011 (accessed on 1 March 2016).
12. Ortega, M. The Bitcoin Transaction Graph Anonymity. Master Thesis, Universitat Oberta de Catalunya, 2013. Available online: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23562/9/msantamariaoTFM0613memoria.pdf (accessed on 1 March 2016).
13. Python. Available online: http://www.python.org/ (accessed on 1 March 2016).
14. BTC-Network Data Scraper. Available online: https://github.com/ivan-brugere/Bitcoin-Transaction-Network-Extraction (accessed on 1 March 2016).
15. Bitcoin Client v0.5.3.1. Available online: https://bitcoin.org/en/release/v0.5.3.1 (accessed on 1 March 2016).
16. Brugere, I. Bitcoin Transaction Network Dataset. Data Set 2013. Available online: http://compbio.cs.uic.edu/data/bitcoin/ (accessed on 1 March 2016).
17. Eclipse SDK Workbench. Available online: http://www.eclipse.org/downloads/ (accessed on 1 March 2016).
18. NetworkX. Available online: http://networkx.github.io/ (accessed on 1 March 2016).
19. MatPlotLib. Available online: http://matplotlib.org/ (accessed on 1 March 2016).
20. PyGraphviz. Available online: http://networkx.lanl.gov/pygraphviz/index.html (accessed on 1 March 2016).
21. Gephi. Available online: https://gephi.org/ (accessed on 1 March 2016).
22. Cran-R. Available online: http://www.r-project.org/ (accessed on 1 March 2016).
23. Cran-R Spatial Data Package. Available online: http://cran.r-project.org/web/packages/sp/index.html (accessed on 1 March 2016).
24. Cran-R Maptools Package. Available online: http://cran.r-project.org/web/packages/maptools/index.html (accessed on 1 March 2016).

25. Cran-R RColorBrewer Package. Available online: http://cran.r-project.org/web/packages/RColorBrewer/index.html (accessed on 1 March 2016).
26. Gross, J.; Yellen, J. *Handbook of Graph Theory*; CRC Press LLC: Boca Raton, FL, USA, 2004.
27. Nykamp, D.Q. The Degree Distribution of a Network. 2013. Available online: http://mathinsight.org/degree_distribution (accessed on 1 March 2016).
28. Albert, R.; Barabasi, A.-L. Statistical Mechanics of Complex Networks. *Rev. Mod. Phys.* **2002**, *74*, 47. [CrossRef]
29. Clegg, R. Power Laws in Networks, Lecture, University of York, 2006. Available online: http://www.richardclegg.org/networks2/SpecialLecture_06.pdf (accessed on 1 March 2016).
30. Newman, M.E.J. The Structure and Function of Complex Networks. *SIAM Rev.* **2006**, *45*, 167–256. [CrossRef]
31. Newman, M.E.J. Power Laws, Pareto Distributions, Zipf's Law. *Contemp. Phys.* **2005**, *46*, 323–351. [CrossRef]
32. Barabasi, A.-L.; Albert, R.; Jeong, H. Scale-free Characteristics of Random Networks: The Topology of the World-Wide Web. *Phys. A* **2000**, *281*, 2069–2077.
33. Inaoka, H.; Ninomiya, T.; Taniguchi, K.; Shimizu, T.; Takayasu, H. Fractal Network Derived from Banking Transaction—An Analysis of Network Structures Formed by Financial Institutions. 2004. Available online: https://www.boj.or.jp/en/research/wps_rev/wps_2004/data/wp04e04.pdf (accessed on 1 March 2016).
34. Saramäki, J.; Kivela, M.; Onnela, J.-P.; Kaski, K.; Kertesz, J. Generalizations of the Clustering Coefficient to Weighted Complex Networks. *Phys. Rev. E* **2007**, *75*, 027105. [CrossRef] [PubMed]
35. Watts, D.; Strogatz, S. Collective Dynamics of Small-World Networks. *Nature* **1998**, *393*, 440–442. [CrossRef] [PubMed]
36. Mao, G.; Zhang, N. Analysis of Average Shortest-Path Length of Scale-Free Network. *J. Appl. Math.* **2013**. [CrossRef]
37. Freeman, L. Centrality in Social Networks Conceptual Clarification. *Soc. Netw.* **1979**, *1*, 215–239. Available online: http://leonidzhukov.ru/hse/2013/socialnetworks/papers/freeman79-centrality.pdf (accessed on 1 March 2016). [CrossRef]
38. Bonacich, P. Power and Centrality: A Family of Measures. *Am. J. Sociol.* **1987**, *92*, 1170–1182. [CrossRef]
39. Borgatti, S. Centrality and Network Flow. *Soc. Netw.* **2005**, *27*, 55–71. [CrossRef]
40. Yan, E.; Ding, Y. Applying Centrality Measures to Impact Analysis: A Coauthorship Network Analysis. 2010. Available online: http://arxiv.org/pdf/1012.4862.pdf (accessed on 1 March 2016).
41. Newman, M.E.J. A measure of betweenness centrality based on random walks. *Soc. Netw.* **2005**, *27*, 39–54. Available online: http://arxiv.org/pdf/cond-mat/0309045.pdf (accessed on 1 March 2016). [CrossRef]
42. Brugere, I. Bitcoin tools. Available online: https://github.com/ivan-brugere/Bitcoin-Transaction-Network-Extraction (accessed on 1 March 2016).
43. Blockchain.info. Blockchain Data API. Available online: https://blockchain.info/de/api/blockchain_api (accessed on 1 March 2016).
44. Bitcoin Charts. Historical Trade Data. Available online: http://bitcoincharts.com/charts/mtgoxUSD#igDailyzczsg2010-07-17zeg2013-12-23ztgSzm1g10zm2g25zv (accessed on 1 March 2016).
45. Bitcoin Talk Forum. Available online: https://bitcointalk.org/ (accessed on 1 March 2016).
46. Alstott, J. Powerlaw: A Python Package for Analysis of Heavy-Tailed Distributions. 2014. Available online: http://arxiv.org/pdf/1305.0215v3.pdf (accessed on 1 March 2016).

1. Introduction

It is not ironic that Milton Friedman, author of a leading treatise on the interaction of currency, macroeconomics and governmental action[1] prophesized of a time when the internet would help evolve a new currency.

Most of the currencies in the world at present, including the reserve currencies, are fiat currencies.[2] The term 'fiat currencies' refers to currencies that are issued by a government, and the government promises to pay the holder of such currencies an equivalent amount in gold, if needed.[3] Thus, these currencies usually have a central regulatory body which issues them, and are consequently called 'centralized'. In fact, at the end of the day, they have the value they have, because somebody said so.[4] The modern state can make anything it chooses as acceptable currency, without any further backing of any kind, even without a connection with gold.[5]

A cryptocurrency is a medium of exchange that uses cryptography to manage the creation of new units as well as secure the transactions.[6] These are a subset of digital currencies.[7] One of the most striking features of cryptocurrency is that it weeds out the need for a trusted third party such as a governmental agency, bank etc. The cryptocurrency system collectively creates the units. The rate at which such units are created is defined beforehand and is publicly known[8] unlike the traditional currencies where the government or the authorized banks control the supply. The fundamental system on which most cryptocurrencies are based today was created by Satoshi Nakamoto.[9]

The production of most cryptocurrencies is deigned to gradually decrease, eventually placing a cap on the number of units that will ever be in circulation. This can lead the currency to mimic the scarcity that is usually seen in the supply of precious metal, thus avoiding hyperinflation.[10] The cryptocurrencies today, are pseudo-anonymous, though newer currencies like Zerocoin have been suggested to allow for complete anonymity.[11]

In 2008, in the aftermath of the subprime mortgage crisis, the confidence in the government issued currency and governments' and bank's ability to manage the economy, the supply of money had almost hit rock bottom. Millions of dollars were used to bail out banks and insurance companies after the "quantitative easing" measures adopted by the Federal Reserve. This essentially meant that money was being printed in order to stimulate the economy. The glut of currency backed with little or no economic productivity led to a global recession ultimately precipitating a sovereign debt crisis in several countries. The price of gold was constantly rising. At this point, the paper by Satoshi Nakamoto[12] was published online describing the Bitcoin for the first time. In the opinion of Nakamoto, the major problem with conventional currency today was that trust was required to make the system work. He makes it clear in in his paper, that while looking at the history of fiat currencies, one can see that it is full of breaches of such trust. He further goes on to state that banks use the currency entrusted to them to lend it out in 'waves of credit bubbles', with hardly anything left in reserve.[13]

Thus, Nakamoto's ideologies in creating Bitcoin would seem to be entirely political. Supporting this argument is the fact that he introduced the currency just a few months after the collapse of the global banking sector.[14] His Bitcoin software would allow its users to send money over the internet directly to each other without an intermediary, and no outside

1. A Monetary History of the United States , 1867 – 1960, Milton Friedman and Anna Schwartz, Princeton University Press.
2. Vincent Scheurer, The Magic of Money: Can our current system of fiat money survive in the long term?, The Motley Fool, http://news.fool.co.uk//news/investing/2011/07/01/the-magic-of-money.aspx.
3. Abba P. Lerner, *Money as a Creature of State,* The American Economic Review, 37 (2), 312 (1947).
4. *Incidentally, the term 'fiat' is Latin for "let it be done" or "it shall be"*
5. Abba P. Lerner, *"Money as a Creature of State",* The American Economic Review, 37 (2), 312 (1947).
6. Andy Greenberg (20 April 2011). "Crypto Currency". Forbes.com.
7. Jerry Brito, Houman B. Shadab and Andrea Castillo, Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling, 16 Colum Sci and Tech J
8. Nicholas A. Plassaras, Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF, 14 Chi J Intl L 377 (2013).
9. Jerry Brito and Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers". Mercatus Center. George Mason University.
10. This is Huge: Gold 2.0 - Can code and competition build a better Bitcoin?, New Bitcoin World.
11. Zerocoin' Add-on For Bitcoin Could Make It Truly Anonymous And Untraceable, Forbes, 26 May 2013
12. This name has been used in this paper to refer to the pseudonymous identity of the creator Bitcoin.
13. Taken from a five-hundred word essay written by Satoshi Nakamoto, where Bitcoin were mentioned for the first time. A copy of the essay is available at: http://Bitcoin.org/Bitcoin.pdf
14. Joshua Davis, The Crypto-Currency, The New Yorker, http://www.newyorker.com/reporting/2011/10/10/111010fa_fact_davis.

party could create Bitcoin,[15] entirely cutting out the role of central banks and governments in online transactions. As Nakamoto said, *'everything is based on crypto proof instead of trust'*.[16] Furthermore, unlike banks and governments which can print more money whenever they deem fit, the bots that are currently creating Bitcoin are supposed to stop doing so in or around the year 2140 according to their programming itself.[17] And unlike fiat currencies, whose value is derived through regulation or law and underwritten by the state, Bitcoin derive their value through the simple principles of supply and demand – they have no intrinsic value and no backing, and their value depends entirely on what people are willing to trade for them.

Hence, no faith or trust towards the financers or politicians was required in case of Bitcoin, but only in Nakamoto's well-designed algorithms. Not only the public ledger of Bitcoin, i.e. the 'block chain' seemed to fend off fraud, but also kept the money supply of Bitcoin growing at a predictable rate due to the prearranged release of the virtual currency. The Bitcoin network came into existence with the release of open source Bitcoin client and with the issuance of the first Bitcoin. Satoshi mined[18] the first 50 Bitcoin which are famously known as the "Genesis Block". In the same year the exchange rate of Bitcoin was first published by liberty standard at $1 for 1,309.03 BTC.[19] Within a couple of years, around February 2011, Bitcoin achieved dollar parity and was now being accepted all over the world as a mode of payment for a plethora of products.[20] Even Wikileaks and other organizations started accepting Bitcoin as donations. Although, during the same year, Bitcoin suffered a security breach in one of the largest Bitcoin exchanges, Mt. Gox and crashed. But, it also bounced back being stronger than before. Since then, Bitcoin have been extremely volatile but have not seen any major security breaches.[21]

Nakamoto had created the first working cryptocurrency, making it as different from the existing fiat currencies as possible. It was meant to be an alternative to them, a new method of transaction, entirely free of government control, and, perhaps a challenge to it. It was to challenge the governments, to make people rethink the existing economic systems, to question their faith in it.

This paper examines legal aspects in relation to Bitcoin specifically and as corollary to cryptocurrencies generally and analyses transactions respecting Bitcoin in India.

> *"Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value."*

Eric Schmidt, CEO of Google

15. *Ibid*
16. Taken from a five-hundred word essay written by Satoshi Nakamoto, where Bitcoin were mentioned for the first time. A copy of the essay is available at: http://p2pfoundation.ning.com/forum/topics/Bitcoin-open-source.
17. Benjamin Wallace, The Rise and Fall of Bitcoin, Wired, Nov. 23, 2011,http://www.wired.com/magazine/2011/11/mf_Bitcoin/.
18. For the definition of "Mining", See, https://Bitcoin.org/en/vocabulary#mining
19. *See,* http://stanford.edu/~eaortiz/cs181report/history.html
20. *See,* http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate
21. *See,* www.nytimes.com/interactive/technology/Bitcoin-timeline.html

2. What Is Bitcoin?

Bitcoin is a cryptocurrency, a form of payment that uses cryptography to control its creation and management, rather than relying on central authorities.[22] According to Nakamoto, Bitcoin is a software-based online payment system and introduced as open-source software in 2009.[23] By some, it is also considered to be the world's first decentralized currency ('currency' is used in a loose sense and does not mean fiat currency as stated above).[24] Unlike usual forms of currency, it is in virtual form and may be used to transact in physical as well as online transactions. The origin of the concept of Bitcoin can be traced to Satoshi Nakamoto, who discussed in his research paper the design of Bitcoin as a new digital currency.[25] The idea of a digital currency – expedient and imperceptible, freed from the supervision of banks and the government has been one of the most discussed and strived for ideas since the advent of the modern internet. Many proposals for such a currency were floated but none were successful. In order to understand Bitcoin, it is important to understand the type of financial instrument it represents. Bitcoin, is a peer-to-peer digital system of payment. As Satoshi Nakamoto, the creator of Bitcoin puts it – "an electronic cash system".[26]

Payments are recorded in a public ledger using its own unit of account. When the algorithm was created by Nakamoto, a finite limit of 21 million on the number of Bitcoin that would ever exist was set.[27] Currently, over 12 million are in circulation.[28] The number of Bitcoin mined has skyrocketed since 2009. The system was intended to be set up in a way where the difficulty of mining every next Bitcoin is greater than the previous one. The final Bitcoin will be mined in the year 2140, at the current rate.[29]

Designing of a digital/virtual currency, involves many challenges. One of the most fundamental challenges is that of double spending. Since the unit of this currency is just information, free from physical structures of metal or paper, there is nothing much to keep people from reusing that piece of information more than once. This would result in spending the same unit of currency more than once. The usual answer for such a problem would be to depend on a central clearing house that would keep a real-time record of all transactions done in that particular currency. This would ensure that the same unit of the currency could not be spent again. Although, this solution would prevent fraud, but it would also require a trusted third party for its administration. This was the problem in the first place that led to the birth of Bitcoin. It is clear from Nakamoto's paper that this currency, unlike all the others, was based on math/cryptography and not trust.[30]

To tackle this fundamental but crippling problem faced by the virtual currency, Nakamoto used "block chains". A block chain is a ledger that is shared publicly where all transactions are recorded. This way transactions could be verified and the problem of double spending could be kept under a check. The chronological order and the authenticity of the block chain are also maintained through a process called cryptography.[31] Cryptography is used to protect information by converting it into an unreadable format (encryption), called cipher text. Each such encryption is secured by a unique key. Only those who have the key can decipher the message into plain text (decryption). Sometimes these messages can be accessed by cryptanalysis (code-breaking), although modern cryptography techniques are practically unbreakable. Ordinarily, cryptography systems can be classified into:

i. symmetric-key systems that use a single key that both the sender and recipient have, and

ii. public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

Obtaining Bitcoin

22. Jerry Brito, Andrea Castillo, *"Bitcoin: A Primer for Policymakers"* [2013], available at http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf
23. Satoshi Nakamoto, Bitcoin: "A Peer-to-Peer Electronic Cash System", Bitcoin.org , available at: http://Bitcoin.org/Bitcoin.pdf
24. *See* http://thomsonreuters.com/business-unit/legal/digital-economy/Bitcoin-101.pdf
25. Satoshi Nakamoto, 'Bitcoin: A peer to peer electronic cash system' 2009 http://Bitcoin.org/Bitcoin.pdf
26. Satoshi Nakamoto, 'Bitcoin: A peer to peer electronic cash system' *(IbIbid.) See* also; Plassaras, Nicholas, Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF (April 7, 2013). Chicago Journal of International Law, 14 Chi J Intl L (2013). Available at SSRN: http://ssrn.com/abstract=2248419
27. Benjamin Wallace, *The Rise and Fall of Bitcoin,* Nov. 23, 2011 available at : http://www.wired.com/2011/11/mf_Bitcoin/
28. See, http://www.forbes.com/sites/samanthasharf/2014/01/15/10-one-perspective-on-what-Bitcoin-will-be-worth-in-2014/
29. See, http://www.cnbc.com/id/101332124#.
30. Satoshi Nakamoto, Bitcoin: *A Peer-to-Peer Electronic Cash System,* Bitcoin.org , available http://Bitcoin.org/Bitcoin.pdf.
31. Block Chain, 'My Wallet Be Your Own Bank' <https://blockchain.info/wallet/>

There are three primary ways to obtain Bitcoin:

i. mining new ones.

ii. buying on an exchange; and

ii. accepting them for goods and services.

'Mining' is discovering new Bitcoin. In reality, it's simply the verification of Bitcoin transactions.[32] In order to make sure a Bitcoin is genuine, miners verify the transaction.[33] There are many transactions that individuals are trying to verify and not just one. These transactions are gathered into boxes with a virtual padlock on them which make up the 'block chains'. 'Miners' run software to find the key to open that padlock. Once the computer finds it, the box pops open and the transactions are verified.[34] Hence, it can be said that while Bitcoin are "mined" by individuals, they are "issued" by the software.

A 'centralized' currency system is one where all of the currency is monitored by a central agency.[35] Certain centralized forms of virtual currencies also exist in centralized forms, such as Facebook credits.[36] These are also subject to similar regulation, and are monitored by banks and governments.[37] The central authority makes controlling and monitoring customers and their transactions much easier. Since, money is traditionally centrally regulated, the surge in Bitcoin has invited mixed reactions from regulators across the globe. It has been treated differently in different parts of the world as regards to taxation and other issues.[38] The recent past has seen an enormous growth in Bitcoin as a form of payment. This is because the fee charged in case of making payments with the use of Bitcoin is lower than the general 2-3% interest imposed by credit card processors.[39]

In India, entrepreneurs have shown enthusiasm towards the Bitcoin system and all eyes are on the Reserve Bank of India (RBI), which has not yet come out with an ultimate verdict. Although, RBI has issued a press release cautioning users, holders and traders of Virtual currencies, including Bitcoin, about the potential financial, operational, legal, security related risks that they are exposing themselves to.[40] Pending this, it is also time to think about the tax treatment of Bitcoin as the transactions in virtual currency are increasing in India.[41] According to Nishith Desai, Bitcoin per se are not illegal in India and this is in consonance with an international approach. Bitcoin creation and transfer are based on open source cryptographic protocol managed in a decentralized manner, and, if harnessed properly, Bitcoin could deliver many benefits to the Indian economy.[42]

Today, real currency is being used to purchase and sell Bitcoin at the current exchange value. Once the purchase has been made the value of the particular amount of Bitcoin is transferred from one wallet to another.[43] Since every wallet has its own unique 33 characters and all Bitcoin wallets are synchronized, thus a false entry by any single person being made is almost impossible.[44] Although pseudonyms are used for trading purposes, the history of every transaction in the form of continuously updated block-chain information is stored in the wallets.[45]

32. Ibid.
33. Dean, Andrew, "Online Gambling Meets Bitcoin" available at https://www.moneypot.com/online-gambling-meets-Bitcoin
34. Blocks, BITCOIN WIKI, https://en.Bitcoin.it/wiki/Block
35. Dr. Rhys Bollen, "The Legal Status of Online Currencies: Are Bitcoin The Future? "Journal of Bank.& Fin. L. & Pr., 3, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285247.
36. http://developers.facebook.com/blog/post/2012/06/19/introducing-subscriptions-and-local-currency-pricing/
37. For instance, in the US, the FinCEN has extended its regulations to Virtual Currencies, thus requiring agencies like Facebook which issue virtual currencies to monitor their customers and their transactions; FinCen, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, available at: http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.
38. See, http://www.livemint.com/Money/3qcKrBcAMIisahVOyOygYK/Are-Bitcoin-currency-or-asset.html
39. A. Rogojanu and L. Badea, "The issue of competing currencies.Case study – Bitcoin"; Theoretical and Applied Economics Volume XXI (2014), No. 1(590), pp. 103-114.
40. *See,* http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247
41. *See,* www.livemint.com/Money/.../Are-Bitcoin-currency-or-asset.html
42. *See,* http://www.thehindu.com/business/Economy/Bitcoin-per-se-are-not-illegal-in-indianishithdesai/article5538900.ece
43. *See,* http://timesofindia.indiatimes.com/tech/tech-news/Trade-in-Bitcoin-gains-currency-among-youth-in-Mumbai/articleshow/27378658.cms
44. *See,* http://www.coindesk.com/meet-tiny-Bitcoin-wallet-lives-skin/
45. *See,* https://blockchain.info/wallet/wallet-faq

3. Applications of Cryptocurrencies

There are a growing number of businesses and individuals using cryptocurrencies like Bitcoin. These include brick and mortar businesses like restaurants, apartments, law firms, and popular online services such as Namecheap, WordPress, Reddit and Flattr. While cryptocurrency remains a relatively new phenomenon, it is growing fast. According to CoinDesk, they are being used in North and South America, Europe, Africa, and Asia.[46] The number of companies accepting Bitcoin has also soared in the past year.[47]

Bitcoin is steadily increasing in popularity as an accepted currency all around the world. The primary areas of Bitcoin use are by individuals and merchants working in technology; however, the users and uses of Bitcoin are rapidly increasing. Several vendors and marketplaces now accept Bitcoin as a mode of payment. This trend holds particularly true for vendors who accept micropayments, such as payments for digital music downloads. Such vendors value the use of Bitcoin to avoid the transaction costs associated with traditional electronic payment methods. Many other vendors do not accept Bitcoin directly, rather, they use an intermediary to accept Bitcoin payments and convert it into a standard currency. In short, Bitcoin has become a popular method of transacting with vendors of goods and providers of services. Bitcoin is also a popular currency with individuals who protest the U.S. monetary system or government.[48] However, it has been used for nefarious activities as well. This includes donations to illegitimate organizations, such as the infamous site, Silk Road.[49] Bitcoin is also growing rapidly in the area of online gambling.[50] The growing use of Bitcoin as a standard currency gives rise to a host of potential income tax and other regulatory issues. Unfortunately, the current state of the law fails to provide insight as to what the proper treatment of these Bitcoin transactions should be.[51]

One of the ways to classify virtual currencies is to study its interactions with the fiat money in circulation. This can happen in two ways: a. currency flow through exchanges; and b. flow of currency due to purchasing and sale of real goods and services. The following three types of schemes can be distinguished on this basis:

i. Closed virtual currency scheme:

This type of scheme has minimal link to the actual economy and is occasionally called "in-game only" scheme. In this scheme, a subscription fee is paid by the user to earn virtual currency by performing specified online tasks. This currency can only be used to buy virtual goods and services within such community.

ii. Virtual currency schemes with unidirectional flow:

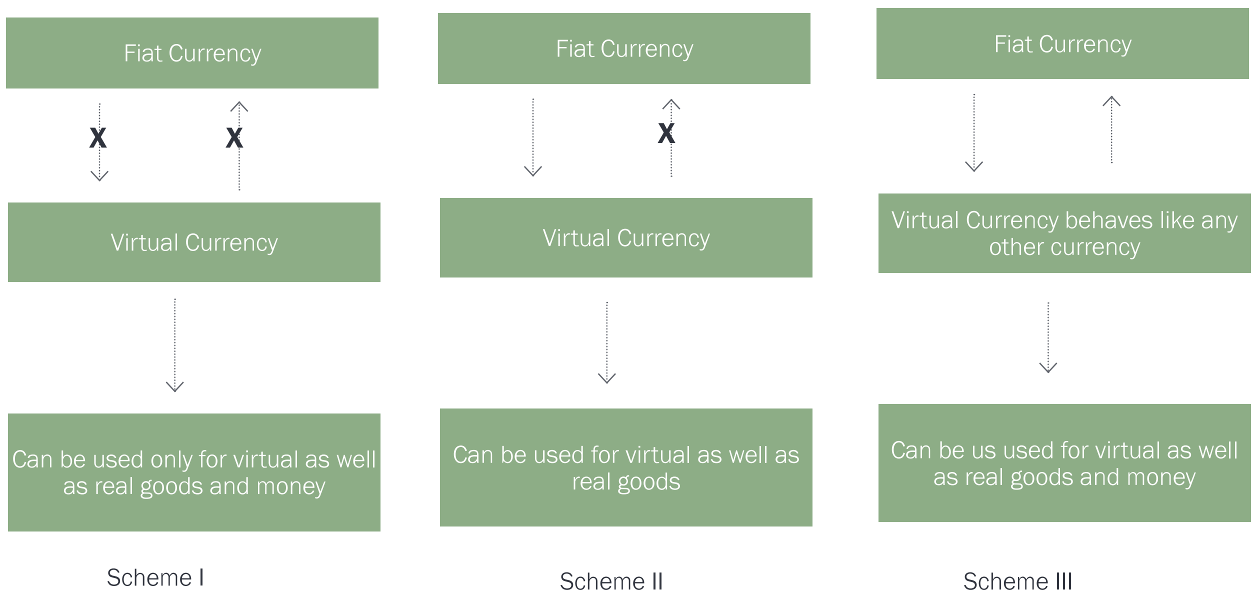
In this scheme real currency is used directly to purchase the virtual currency at a specified rate (exchange rate). Real goods and services may be bought in such a scheme using the virtual currency.

iii. Virtual currency schemes with bidirectional flow:

In this case the virtual currency resembles any other currency capable of exchange. The currency can even be bought and sold according to the set exchange rates. Real as well as virtual goods and services can be bought and sold through this currency. Bitcoin and most other currencies follow this scheme.

The following diagrams depict the flow of fiat and virtual currencies as explained in the schemes above:

46. http://www.coindesk.com/data/bitcoin-total-circulation/
47. http://www.coindesk.com/information/what-can-you-buy-with-Bitcoin/
48. Akins, Benjamin W. and Chapman, Jennifer L. and Gordon, Jason M.,"A Whole New World: Income Tax Considerations of the Bitcoin Economy" Pittsburgh Tax Review. Available at SSRN: http://ssrn.com/abstract=2394738
49. Ibid.
50. http://www.coindesk.com/the-wild-world-of-Bitcoin-and-gambling/
51. Ibid.


Fiat Currency
X
X
Virtual Currency
Can be used only for virtual as well as real goods and money
Scheme I
Fiat Currency
X
Virtual Currency
Can be used for virtual as well as real goods
Scheme II
Fiat Currency
Virtual Currency behaves like any other currency
Can be us used for virtual as well as real goods and money
Scheme III

4. General Position and View Around the World

After the glorious comeback of Bitcoin after the crash of 2011, and its constant growing popularity, it has received much attention from various jurisdictions around the world.[52] Central banks and governments of many nations have issued official statements, regulation and reports on handling of Bitcoin and other significant uses with regard to effecting business transactions. Governments have issued such statements on a wide range of topics from concerns regarding fraud, tax considerations, possibility of negative impacts on national currencies to whether Bitcoin are recognized as legal tender/currency.

It must be noted that this debate over how to deal with this new virtual currency is still in its infancy. Also, the characterization of Bitcoin as currency has been rejected by most jurisdictions which have taken steps to regulate it. The major reason for doing so seems that they would not want to confer such a status to peer-to-peer units. Certain countries like China[53] and Brazil[54] have made efforts to warn people of the risks associated with trading in Bitcoin. RBI too has issued a similar caution. Several nations such as Canada, [55]Norway[56] and Singapore [57] have declared Bitcoin as 'assets'. Although, it may be noted that such an approach might lead to several difficulties. For instance, once Bitcoin have been mined by a party, the transfer of these Bitcoin may not be subjected to capital gains tax, if treated in a similar manner as the self-acquired tangible assets.[58]

Virtual currencies have also not been covered under the exceptions that have been carved out in some specific types of transactions with regard to sale of self-generated assets in cases where Bitcoin are characterized as assets. Payments to contractors and sub-contractors, the whole of which may not be characterized as income or profits in the hands of the recipient, may not be subject to withholding obligations where Bitcoin are characterized as assets.[59] "The following is an analysis of specific statements/rules/regulations published by governments of various nations specifically addressing the issue of Bitcoin."

I. Australia

The Australian Taxation office (ATO) had informed that it was keeping a close watch on the "volatility [of Bitcoin], how widely it is accepted, its interaction with conventional currencies through exchange mechanisms and international developments". A Draft ruling of Goods and services tax (GST), a guidance paper and four tax determinations on the taxation treatment of Bitcoin and other virtual currencies were also issued in august 2014.[60]

In October 2013, an Australian Bitcoin bank was hacked, resulting in the theft of over US$1 million worth of the Bitcoin.[61]

II. Brazil

Through Law No. 12865, enacted by Brazil on October 9, 2013, the possibility for creation of electronic/virtual currencies, including Bitcoin, was introduced. Among other things the law laid down the kind of payment systems and payment arrangements that are included in the Brazilian Payment System (*Sistema de Pagamentos Brasileiro,*

52. *See,* http://www.economist.com/node/21563752
53. Banks and payment institutions in China are thus prohibited from dealing in Bitcoin. China Bans Financial Companies From Bitcoin Transactions, BLOOMBERG NEWS (Dec. 5, 2013), available at : http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financialcompanies-from-Bitcoin-ransactions.html; [Notice on Precautions Against the Risks of Bitcoin] (issued by the People's Bank of China, the Ministry of Industry and Information Technology, China Banking Regulatory Commission, China Securities Regulatory Commission, and China Insurance Regulatory Commission, Dec. 3, 2013) YIN FA, 2013, No. 289, http://www.pbc.gov.cn/publish/goutongjiaoliu/524/2013/20131205153156832222251/20131205 153156832222251_.html (China).
54. *See,* http://www.bcb.gov.br/pt-br/Paginas/bc-esclarece-sobre-os-riscos-decorrentes-da-aquisicao-das chamadas-moedas-virtuais-ou-moedas-criptografadas.aspx
55. Jasper Hamill, "Canadian Regulators Welcome US Bitcoin Refugees with Open Arms", REGISTER (May 20, 2013), available at: http://www.theregister.co.uk/2013/05/20/canada_welcomes_Bitcoin_traders_fintrac_letter/.
56. *See,* http://www.bloomberg.com/news/2013-12-12/Bitcoin-fail-real-money-test-in-scandinavia-s-wealthiest nation.html
57. *See,* http://www.forbes.com/sites/kellyphillipserb/2014/03/25/irs-says-Bitcoin-other-convertible-virtual currency-to-be-taxed-like-stock/
58. *See,* http://www.livemint.com/Money/3qcKrBcAMIisahVOyOygYK/Are-Bitcoin-currency-or-asset.html
59. *See,* http://www.livemint.com/Money/3qcKrBcAMIisahVOyOygYK/Are-Bitcoin-currency-or-asset.html
60. Kate Walsh & Jason Murphy, ATO Targets Bitcoin Users, AUSTRALIAN FINANCIAL REVIEW (June 24, 2013), http://www.afr.com/p/technology/ato_targets_Bitcoin_users_oawpzLQHDz2vEUWtvYLTWI.
61. Jim Urquhart, Bit-Heist: Over $1mn in Bitcoin Stolen from Australian Online Bank, RT.COM (Nov. 8, 2013), http://rt.com/news/Bitcoin-hacking-stolen-million-417/.

SPB).[62] "Payment institution" is defined as a legal entity that, by adhering to one or more payment arrangements, has as a principal or secondary activity, alternatively or cumulatively, one of the activities listed in article 6(III). "Electronic currency" is defined as resources stored on a device or electronic system that allow the end user to perform a payment transaction.[63]

III. China

The central bank of China and four other central government ministries and commissions, issued a Notice on Precautions against Risks of Bitcoin in December 2013.[64] The notice clearly stated that the nature of Bitcoin is that of a "virtual commodity" and not a currency. Owing to this fact, Bitcoin should not be traded as a currency in the market.[65] The notice also prohibited the Financial Institutions in China from dealing in Bitcoin. The notice further mentioned that overseeing of internet sites that dealt in services relating to the Bitcoin was to be made much more stringent. It also issued a general warning issues relating to money laundering with the use of Bitcoin.[66]

IV. Canada

Canada is the first country to implement a national law on Bitcoin use. As a result of recent legislative amendments, businesses dealing in digital currency have now been subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act of 2000 (**"PCMLTF"**). Under the PCMTF, 'dealing in virtual currencies [67]' has been subjected to the same reporting requirements as other money-services businesses.

Dealers in digital currency in Canada need to register as Money Services Businesses (**"MSBs"**). Anyone dealing with customers in Canada will need to register as an MSB with the Financial Transactions and Reports Analysis Centre of Canada (**"FINTRAC"**). The process involves contacting FINTRAC to provide initial information and gaining access to the MSB registration site. There are a number of questions about the owners of the business, senior officers, banking relationships and projected revenues. While the process is not costly, it can take time (in particular if the regulator requires clarification). Some of the reportings / filings that will need to be made to FINTRAC are[68]:

- Digital Currency MSBs are required to report to FINTRAC every suspicious financial transaction and attempted suspicious financial transaction. There is no monetary threshold (i.e., dollar amount) that triggers the requirement to report a suspicious transaction.
- Digital Currency MSBs have to file with FINTRAC, a terrorist property report when it has property in its possession or control that it knows is owned or controlled by or on behalf of a terrorist or terrorist group; and when it has property in its possession or control that it has reason to believe is owned or controlled by or on behalf of a listed person.
- Digital Currency MSBs are required to report to FINTRAC when they receive an amount of $10,000 or more in cash in the course of a single transaction, unless the funds are received by a public body or a financial entity.

When a Digital Currency MSB sends or receives an international money transfer of $100,000 or more, it must determine if it involves a politically exposed person (**"PEP"**) inside or outside of Canada, and if it determines that the funds involve a PEP, it must confirm the source of funds.

- Digital Currency MSBs have to undertake obligations to ascertain the identity of persons and companies using their services to complete certain financial transactions.
- Digital Currency MSBs are subject to fairly onerous record-keeping obligations under the PCMLTFA. They must keep large cash transaction records, records regarding third parties when certain transactions are conducted for third parties.

62. Lei No. 12.865, de 9 de Outubro de 2013 [Law No. 12,865 of October 9, 2013], http://www.receita.fazenda.gov.br/Legislacao/leis/2013/lei12865.htm (Braz.).
63. Ibid. Article 6 (VI)
64. 关于防范比特币风险的通知 [Notice on Precautions Against the Risks of Bitcoin] (issued by the People's Bank of China, the Ministry of Industry and Information Technology, China Banking Regulatory Commission, China Securities Regulatory Commission, and China Insurance Regulatory Commission, Dec. 3, 2013) Yin Fa, 2013, No. 289,http://www.pbc.gov.cn/publish/goutongjiaoliu/524/2013/20131205153156832222251/20131205153156832222 251_.html (China). An unofficial English summary of the Notice is available at BTC CHINA, https://vip.btcchina. com/page/bocnotice2013 (last visited Jan. 5, 2015).
65. Ibid. Section 1
66. Ibid
67. The phrase "dealing in virtual currencies" was not defined and it is not known what the defined term will encompass in terms of transactions but the government has clarified that it will apply only to digital currency exchanges.
68. http://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/

- Digital Currency MSBs have to undertake a risk assessment to evaluate and identify, in the course of its activities, the risk of the commission of money laundering offences and terrorist activity financing offenses.
- Digital Currency MSBs are required to implement a compliance program to meet reporting, record keeping and client identification obligations under the PCMLTFA.

Failures to comply with certain obligations under the PCMLTFA are criminal offences and can subject directors, officers, employees and the Digital Currency MSB to terms of imprisonment and fines. Digital Currency MSBs should obtain compliance advice in respect of their exposure and should understand the connection in Canada between the compliance regime and a due diligence defence.

In April 2013, Canada's Revenue Agency (**"CRA"**) reportedly stated that users of bitcoins will have to pay tax on transactions in the digital currency, based on two separate tax rules that apply to barter transactions and things that are bought and sold for speculative purposes. These rules were confirmed in November, 2013. In essence, the matter will be dealth with on a case by case basis. Under Canadian law, barter transactions are allowed, but the CRA states that the value of goods or services obtained by bartering digital currencies must be included into the taxpayer's income, if business related.[69]

V. Denmark

The Financial Supervisory Authority (Denmark's *Finanstilssynet*) in addition to stating that it will not be regulating Bitcoin, clarified the status of Bitcoin stating that it was not a currency.[70] In the same statement it was explained that since Bitcoin did not fall under any kind of financial services categories, including electronic money, currency exchanges etc., it cannot be covered under the financial regulation.[71]

This statement by the Financial Supervisory Authority suggests that Bitcoin should be treated as an electronic service and earnings from its use would therefore be taxable. However, the tax authorities have not published any comment yet as to whether Bitcoin earnings should be or will be taxed. Even though there is no clarification from the tax authorities regarding taxation of the Bitcoin, the Danish Tax Authority (SKAT) published a reply wherein it stated that an invoice cannot be issued in Bitcoin but must instead be issued in Danish Kroner or another recognized currency. It was also stated that losses in Bitcoin could not be deducted as a cost of business.[72] Hence, currently, although it is clear that Bitcoin is not a recognized currency, there still is some lack of clarity with regard to the taxability of Bitcoin under the jurisdiction.

VI. European Union

No legislation yet has been passed by the EU relating to the status of Bitcoin as a currency. A detailed report on virtual currency which discussed the Bitcoin system and briefly analyzed its legal status within the EU was issued by the European Central Bank.[73] However in the conclusion of the report, the Bitcoin was kept outside the purview of directive 2007/64/EC since the directive does not deal with electronic money and the financial institutions are not allowed to deal in it either.[74] In December 2013, European Banking Authority (EBA), the regulatory and advisory agency of the EU in matters of banking institutions, e-money regulation etc. issued a warning on the dangers of using virtual currency. It also clarified that the consumers might still be taxed when using virtual currency as Bitcoin is not regulated.[75]

VII. Germany

BaFin *(BundesamtfürFinanzdienstleistungenissued)*, the German Federal Financial Supervisory Authority issued a communication on Bitcoin on December 19, 2013.[76] In Germany Bitcoin have been classified as a

69. http://www.coindesk.com/information/is-bitcoin-legal/
70. Advarsel mod virtuellevalutaer (Bitcoinm.fl.) [Warnings Against Digital Currencies (Bitcoin etc.)], Finanstilsynet (Dec. 17, 2013), http://www.finanstilsynet.dk/da/Nyhedscenter/Pressemeddelelser/2013/Advarsel-mod-virtuelle-valutaer-bitcom-mfl-2013.aspx.
71. Ibid.
72. European Central Bank, Virtual Currency Scheme http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.
73. Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market, Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and Repealing Directive 97/5/EC, 2007 O.J. (L 319) 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319: 0001:0036:EN:PDF
74. Press Release, European Banking Authority, EBA Warns Consumers on Virtual Currencies (Dec. 13, 2013),http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies.
75. Jens Münzer, Bitcoin: AufsichtlicheBewertung und RisikenfürNutzer [Bitcoin: Supervisory Evaluation and Risks for Users], BaFin http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/ 2014/fa_bj_1401_Bitcoin.html.
76. Kreditwesengesetz [Banking Act] (updated Sept. 9, 1998), Bundesgesetzblatt I at 2776, as amended, See http://www.gesetze-im-internet.de/kredwg/index.html (Ger.).

financial instrument but not any form of currency.[77] The Federal Ministry of Finance discussed briefly the tax treatment of Bitcoin in some statement. The ministry, among other things, discussed the possibility of levying value-added tax liability for Bitcoin transfers, lack of long term capital gains liability for Bitcoin that are held for more than a year.[78]

VIII. Norway

A principle statement was issued by the Norwegian Tax Authority stated that as far as the question of taxation of Bitcoin is concerned, it will be treated as capital gains. The legislation governing the capital property imposes taxes on winnings and deductions for losses. Even though travelling currencies are exempted from the capital gains tax, Bitcoin cannot be exempted as it is not covered under travelling currencies. In addition to this, a commercial sale of Bitcoin will attract 25% of VAT.[79]

IX. United Kingdom

The Bank of England has published no statement clarifying its position on Bitcoin. Although, Bitcoin has been expressly excluded in the latest quarterly reports published.[80] It has been indicated by the HMRC (The UK customs and tax department) that Bitcoin will be considered as 'single purpose vouchers'.[81] This classification will render a levy of VAT extending up to 10-20% on the sale of Bitcoin. This move has been vehemently criticized by those involved in the sale of Bitcoin alleging that this would lead to a tremendous slowdown in the UK Bitcoin industry.[82]

X. United States of America (USA)

A bill submitted to the Congress called HR 5777, proposed a five-year moratorium on regulation of digital currency within the US. The bill is titled "The Crypto-currency Protocol Protection and Moratorium Act" and would hold off any "statutory restrictions or regulations" for a period of five years after 15th June 2015.[83] The draft law also proposes that virtual currencies be classified as traditional currencies under tax regulations of the US. Currently, the Internal Revenue Service ("**IRS**") taxes Bitcoin holdings as though they were a type of property. The moratorium bill contains legislative language that implies that the IRS should be treating Bitcoin and distributed ledger systems as currencies rather than assets.[84] The bill criticizes the current property-focused tax perspective, arguing that it fails to address the multifaceted characteristics of cryptocurrency. The bill, if passed, would require the IRS to revisit and rework its current regulatory framework regarding digital currencies.[85]

As already said, IRS currently treats Bitcoin as "property" for tax purposes. According to the IRS, the classification means that:[86]

- Digital currency payments made to independent contractors and service providers must be reported via Form 1099.
- Profits and losses from the sale of digital currencies are subject to capital gains when being used as capital assets.
- Wages paid to employees in digital currencies are taxable and must be reported.

According to IRS, only US bills and coins have legal tender status in the United States so Bitcoin simply defaults to property status since it's not legal tender. It's ironic that Bitcoin is used as a currency but taxed like property.[87] Presently, there are no final rules at the US state level yet. In March, 2014, the New York State Department of Financial Services had

77. Franz Nestler, Deutschland erkenntBitcoinals privates Geld an [Germany Recognizes Bitcoin as Private Money], Frankfurter AllgemeineZeitung , http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-deutschland-erkennt-Bitcoin-als-privates-geld-an-12535059.html.
78. See, http://www.skatteetaten.no/no/ Radgiver/Rettskilder/Uttalelser/Prinsipputtalelser/Bruk-av-Bitcoin--skatte--og-avgiftsmessige-konsekvenser/.)
79. Mona Naqvi & James Southgate, Bank of England, Banknotes, Local Currencies and Central Bank Objectives, 53: 4 Quarterly Bulletin 319 n. 3 (2013), http://www.bankofengland.co.uk/ publications/Documents/quarterlybulletin/2013/qb1304.pdf.
80. Pete Rizzo, "UK Eliminates Tax on Bitcoin Trading, Publishes Official Guidance", available at http://www.coindesk.com/top-uk-tax-agency-eliminate-20-levy-Bitcoin-trading/
81. Tom Gullen, The Challenge of Being a Bitcoin Trader, Financial Services Club Blog (Nov. 13, 2013),http://thefinanser.co.uk/fsclub/2013/11/the-challenge-of-being-a-Bitcoin-trader.html.
82. http://www.coindesk.com/proposed-us-moratorium-Bitcoin-regulation/
83. http://www.coindesk.com/us-congressman-submit-Bitcoin-tax-bill/
84. http://www.coindesk.com/proposed-us-moratorium-Bitcoin-regulation/
85. http://www.coindesk.com/internal-revenue-service-treat-digital-currencies-property/
86. http://www.wallstreetandtech.com/compliance/Bitcoin-taxation-a-gift-from-the-irs-and-the-coffee-problem/a/d-id/1318419?_mc=RSS_WST_EDT
87. "In the Matter of Virtual Currency Exchanges". Public Order. New York State Department of Financial Services. 11 March 2014. Retrieved 30 March 2014.

officially invited Bitcoin exchanges to apply with them, and published draft regulations for virtual currency businesses. Businesses would have to provide transaction receipts, disclosures about risks, policies to handle customer complaints, maintain a cyber-security program, hire a compliance officer and verify details about their customers to follow anti-money-laundering rules, per FinCEN.[88]

AB 129 has been signed into law in June 2014 to take effect in 2015. The bill was meant to repeal the law that renders illegal, any use of alternative currencies. Other types of alternative currencies besides Bitcoin that now fall within the purview of AB 129 include gift cards, reward points such as are used at shopping malls and virtual tokens.[89] For the purposes of taxation, the IRS in the US considers Bitcoin as 'property' and not currency. However, it was recently ruled by a District Court of Eastern District of Texas[90] that Bitcoin, is in fact a form of currency or money.[91]

XI.Thailand

The Bank of Thailand was given a presentation about how the currency works in a bid to operate in the country. At the end of the meeting, senior members of the Foreign Exchange Administration and Policy Department advised that due to lack of existing applicable laws, controls on capital and the fact that Bitcoin affects more than one financial sphere; the following Bitcoin activities are illegal in Thailand: [92]

i. buying Bitcoin

ii. selling Bitcoin

iii. buying any goods or services in exchange for Bitcoin

iv. selling any goods or services for Bitcoin

v. sending Bitcoin to anyone located outside of Thailand

vi. receiving Bitcoin from anyone located outside of Thailand

However, according to a letter from the Bank of Thailand, it is declared that Bitcoin can be traded in Thailand so long as it's only converted to/from Thai baht. Therefore, Bitcoin cannot be used as a way of converting foreign currencies in the nation. Bank of Thailand says it has no plans to expand the laws to regulate Bitcoin.[93]

In the UK, the Financial Conduct Authority has stated that Bitcoin are not recognized as a currency within the jurisdiction. Countries such as Germany[94] and the UK[95] have attempted to extend value-added taxation ("**VAT**") laws to Bitcoin transactions and it is possible that in the future India might include barter transactions in goods within the newly proposed Goods and Services Tax regime.[96] Bitcoin have not been made illegal in china but financial institutions have been prohibited from dealing directly in them.[97] Monetary Authority of Singapore (MAS) maintains that virtual currencies are not regulated in Singapore.[98] While the MAS has warned speculators about trading in cryptocurrencies, it has also said that the choice to accept Bitcoin is a commercial decision in which the MAS will not intervene.[99] Hence, it is easy to see that the status of Bitcoin within the economies of various jurisdictions is far from settled.

"I understand the political ramifications of [Bitcoin] and I think that government should stay out of them and they should be perfectly legal."

Ron Paul, Republican Texas Congressman and former candidate for US President

88. https://www.cryptocoinsnews.com/ab-129-california-legally-approves-use-bitcoin/
89. https://ia800904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf
90. Vaneesa Abhishek, "Growing interest in Bitcoin: Time for India to welcome it as "currency"?, available at http://articles.economictimes.indiatimes.com/2014-06-18/news/50678868_1_currency-notes-Bitcoin-satoshi-nakamoto
91. "Bitcoin banned in Thailand". Telegraph UK. 13 July 2013. Retrieved 16 December 2013.
92. "Bank of Thailand says country's top Bitcoin exchange can resume operations". Techinasia. 17 February 2014. Retrieved 27 February 2014.
93. See,http://web.bundesverband-Bitcoin.de/wp-content/uploads/2014/05/Press-Release-Bundesverband Bitcoin-PM-14-002_eng.pdf
94. This approach was put forward in HRMC, Tax treatment of activities involving Bitcoin and other similar cryptocurrencies, Revenue & Customs Brief 09/14, (3 Mar. 2014), available at :http://www.hmrc.gov.uk/briefs/vat/brief0914.htm (accessed 25 July 2014).
95. See, https://www.law.ufl.edu/flalaw/wp-content/uploads/2014/03/73TI0971.pdf
96. Gerry Mullany, "China Restricts Banks' Use of Bitcoin," The New York Times, (December 5, 2013). Available at: http://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from usingBitcoin.html.
97. Terence Lee, "Singapore Government Decides Not to Interfere with Bitcoin," TechinAsia (Dec. 23, 2013), available at: http://www.techinasia.com/singapore-government-decides-interfere-Bitcoin/.
98. See, http://www.moneysense.gov.sg/understanding-financial-products/investments/consumer-alerts/virtual-
99. I.R. Coelho v. State of Tamil Nadu (2007) 2 SCC 1.

5. Position in India

I. What is Bitcoin?

The Constitution of India provides for matters in respect of which the Central Government has powers to regulate and legislate. To understand if Bitcoin are capable of government review, an analysis of the Indian Constitution has been undertaken. In this regard, Article 246 read with Seventh Schedule of the Constitution enumerates the list of activities that the Central Government and the State Governments are allowed to legislate.

Entry 36 and 46 of List I of the Seventh Schedule of the Constitution states that the Central Government is allowed to legislate in respect of currency, coinage, legal tender, foreign exchange and bills of exchange, cheques, promissory notes and other like instruments respectively.

If Bitcoin (as discussed below) falls within the purview of any of the above outlined categories of instruments, then the Central Government would have exclusive powers to legislate.

In the hierarchy of laws, the Constitution is supreme. All laws are subordinate to the Constitution. A law may be struck down as being unconstitutional due to lack of legislative competence or because it violates fundamental rights.[100] Decisions of the Union or State Executive, including decisions of statutory authorities, constitutional functionaries and quasi-judicial authorities may be challenged in a State High Court under the Constitution. Rules, regulations, notifications and circulars passed by authorities under the relevant statute may also be challenged on the ground that the same violate the Constitution.

The Constitution empowers, and the Supreme Court of India (“**Supreme Court**”) has recognized, authorities created under a statute to delegate certain functions to subordinate authorities.[101] To facilitate in the effective implementation of government policies certain executive authorities have the power to pass rules and regulations which have the force of law. These rules and regulations are subordinate to the parent law and cannot transgress the limits set out by the parent law. Rules and regulations cannot confer excessive discretion on subordinate authorities.

It is also settled law that authorities acting in furtherance of a statute must carry out their functions in a manner that best achieves the objectives of the statute. These principles are designed to reduce the scope of discretion and eliminate arbitrariness in executive action. Ordinarily, decisions of these authorities may be challenged in appeal before an appellate authority. However, in exceptional circumstances, where there is an egregious violation of fundamental rights, principles of natural justice or when an authority acts in violation of its jurisdiction, an aggrieved party may file a petition in the State High Court.

It is important to note that while challenging the decision of a statutory authority, generally the scope of appeal is limited and there is a high degree of deference by courts. The Supreme Court has recognized that in matters relating to economic policy, courts must not interfere unless arbitrariness is writ large in the decision making process. Even in cases where intervention of the court is justified, the court would only examine the decision making process and not the decision itself.

The principal laws concerning Bitcoin are:

i. The Constitution of India, 1950;

ii. The Foreign Exchange Management Act, 1999 (“**FEMA**”);

iii. The Reserve Bank of India Act, 1934 (“**RBI Act**”);

iv. The Coinage Act, 1906 (“**Coinage Act**”);

v. The Securities Contracts (Regulation) Act, 1956 (“**SCRA**”);

vi. The Sale of Goods Act, 1930 (“**Sale of Goods Act**”); and

vii. The Payment and Settlement Systems Act, 2007 (“**Payment Act**”).

viii. Indian Contract Act, 1872 (“**Contract Act**”)

II. FEMA, RBI and Coinage Act

The three statutes together define and regulate the issuance, utilization and disposal of currencies (and money). The terms legal tender and bank notes have not been clearly defined in any of the three aforementioned statutes. However, from an analysis of the provisions of the relevant regulatory statute, the nature and characteristics of the terms legal tender and bank notes have been determined.

100. Gwalior Rayon Silk Manufacturing (Weaving) Company Ltd. V. Asst. Comm. Sales Tax (1974) 2 SCR.

101. Section 2(h) of The Foreign Exchange Management Act, 1999

III. Currency

The RBI Act does not specifically define currency, but it does define foreign currency to have the same meaning as in Foreign Exchange Regulation Act, 1973, which has since been replaced by FEMA.

'Currency' has been defined under FEMA to include, 'all currency notes, postal notes, postal orders, money orders, cheques, drafts, travelers cheques, letters of credit, bills of exchange and promissory notes, credit cards or such other similar instruments, as may be notified by the Reserve Bank'.[102] FEMA defines 'foreign currency' as any currency other than Indian currency.[103] Definition of 'Indian Currency' under FEMA states that Indian currency is the currency which is expressed or drawn in Indian Rupees. The definition excludes special bank notes and special one rupee issued under section 28A of the RBI Act.[104]

IV. Legal Tender

Although there is no definition for legal tender under Indian law, the power to issue bank notes vests exclusively with the Reserve Bank of India ("**RBI**"). The bank note issued by RBI is considered legal tender (S. 26 of RBI Act).

For any instrument to qualify as a legal tender it must fulfill the test prescribed in Section 13 of the Coinage Act which states that coins issued under the authority of Section 6 of the Coinage Act, shall be legal tender in payment or on account i.e. provided that a coin has not been defaced and has not lost weight so as to be less than such weight as may be prescribed.

Over a period of time various instruments have been defined to mean legal tender, such as One Rupee issued under Currency Ordinance, 1940 as well as bank notes issued by RBI under the RBI Act.

From the above, it could be argued that so far as Bitcoin are not specifically designated by the government to be legal tender, they should not fall within this category.

V. Currency Notes

The term currency notes are specifically defined in Section 2(i) of FEMA to mean and include cash in the form of coins and bank notes. This definition therefore does not cover Bitcoin which are not issued either under the Coinage Act or RBI Act.

S. 22 of the RBI Act provides that RBI has the sole right to issue bank notes and S. 26 provides that bank notes shall be legal tender in India.

From the above it appears that while Bitcoin have several features of a currency or legal tender it is not bank notes and is consequently not legal tender in India. Accordingly, it is left to be examined if it falls within the purview of securities, derivatives, or commodities.

VI. Virtual Currency

The question at hand is whether a 'virtual currency' such as Bitcoin can be said to come under the purview of the definition of currency above.
The answer to this question can be found in the maxim '*express um facit cessare tacitum*'. The maxim represents the principle 'when there is express mention of certain things, then anything not mentioned is excluded'. The maxim has been recognized by Indian courts and was also relied upon by the Supreme Court in *Shankara Rao Badam & Ors. v. State of Mysore & Anr.*[105] and *Union of India & Anr. v. Tulsiram Patel.*[106] In light of the provisions of the law, it can be reasonably concluded that 'virtual currency' should be considered excluded from the definition of currency. While it may be argued that it may fall under 'such other similar instruments' under Section 2(h), but such 'other instruments' need to be specifically notified by the RBI which is not the case. There is no such declaration in respect of cryptocurrencies in general or Bitcoin in particular. RBI has merely advised the public to be cautious regarding the trading of virtual currencies.[107] Therefore, under the provisions of existing law, Bitcoin are not currency.[108]

102 Section 2(m) of The Foreign Exchange Management Act, 1999

103. Section 2(q) of The Foreign Exchange Management Act, 1999

104. [1969] 3 S.C.R. 1

105. 1985 AIR SC 1416

104. RBI Cautions Users of Virtual Currencies Against Risks, Press Release : 2013-2014/1261 dated December 24, 2013 available at: http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247

105. According to Section 26 of the RBI Act, 1934 bank notes can be considered as "Legal Tender". Further, according to Section 24 of the same only RBI has a power to issue it and no one else. See also Are Bitcoin currency or asset?, note 48 above.

106. 2002 178 ELT 22 S.C

107. Hon'ble Mr. Justice S.B. Sinha's view in Tata Consultancy Services v. State of Andhra Pradesh, 271 ITR 401 (2004).

108. Section 2 of The Sale of Goods Act, 1930

VII. Bitcoin as a Good and a Commodity

The term commodity has not been defined anywhere under the law in India. In the case of *Tata Consultancy Services V. State of Andhra Pradesh*[109], Hon'ble Justice Sinha concurring with the court's view stated that a commodity is generally understood to mean goods of any kind, something of use or an article of commerce.[110] Since Bitcoin are an intangible asset, it leaves open the possibility of being characterized as a commodity under Indian law.

Bitcoin may very well fall under the meaning of "goods" and may be covered under the Sale of Goods Act. The act defines "good" as:

> *"every kind of movable property other than actionable claims and money; and includes stock and shares, growing crops, grass, and things attached to or forming part of the land which are agreed to be severed before sale or under the contract of sale."*[111]

Bitcoin are listed and traded on stock exchanges in various jurisdictions around the world. Some examples are (i) Mt. Gox in Japan (previously one of the most widely exchanges); (ii) BTC China; (iii) BitBox in the United States;(iv) Bitcurex in Poland and (v) Bitsamp in Slovenia. Although there is no formal Bitcoin exchange in India at present there are numerous websites through which Bitcoin can be bought and sold. At present, as many as 23,000 Indians possess e-wallets where their digital currency is stored.[112]

Bitcoin wallets keep a secret piece of data called a "private key" for each Bitcoin address. Private keys are used to sign transactions, providing a mathematical proof that they have come from the owner of the addresses. Thus, it can be stated that, it can be stored and transferred. Therefore, in the light of the above discussion and case law, Bitcoin may be liable to tax.

In *Tata Consultancy Services v. State of Andhra Pradesh* [113], *the Supreme Court stated that, "computer software is intellectual property, whether it is conveyed in diskettes, floppy, magnetic tapes or CD ROMs, whether canned (Shrink-wrapped) or uncanned (customized), whether it comes as part of computer or independently , whether it is branded or unbranded, tangible or intangible; is a commodity capable of being transmitted, transferred, delivered, stored , processed , etc. and therefore as a 'good' liable To sale tax."*

Similarly, Bitcoin being of an incorporeal nature may fall under the ambit of the term "goods".

VIII. Bitcoin as Payment System or Pre-Paid Instrument

The RBI regulates and supervises the payment systems in India under the Payment Act. Bitcoin, though often referred to as the peer-to-peer payment system, cannot clear or settle the payment between the payer and the beneficiary. Thereby it is not to be treated as a 'payment system' under the Payment Act.[114]

In India, pre-paid instruments are regulated by RBI in pursuant of its power conferred under the provisions of Payment Act.[115] The directions issued by RBI stipulate that a pre-paid instrument can be used to discharge any payment obligation equivalent to the value attached to it.[116] On the other hand, Bitcoin need not be traded to discharge payment obligations equivalent to its value. Since the value of a Bitcoin are determined by market speculation, it can be either less or more than the payment obligation it is traded for.[117] Therefore, it cannot be said that the value stored in the instrument represents the value paid by the holders.

109. Hon'ble Mr. Justice S.B. Sinha's view in Tata Consultancy Services v. State of Andhra Pradesh, 271 ITR 401 (2004).

110. Section 2 of The Sale of Goods Act, 1930

111. *See*, http://articles.economictimes.indiatimes.com/2013-08-14/news/41409715_1_Bitcoin-gox-virtualcurrency

112. 271 ITR 401 (2004) (Paragraph 84)

113. Section 2(i) of The Payment And Settlement Systems Act, 2007 reads as follows:

"(i) "payment system" means a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange."

114. Section 18 of The Payment and Settlement Systems Act, 2007

115. Master Circular – Policy Guidelines on Issuance and Operation of Pre-paid Payment Instruments in India *"2.3 Pre-paid Payment Instruments: Pre-paid payment instruments are payment instruments that facilitate purchase of goods and services, including funds transfer, against the value stored on such instruments. The value stored on such instruments represents the value paid for by the holders by cash, by debit to a bank account, or by credit card."* Available at: http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=8993

116. *See*, http://www.forbes.com/sites/nathanlewis/2014/03/06/Bitcoin-proves-friedmans-big-plan-was-a-joke/

117. *See*, http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1902

Further, Bitcoin can be generated by a user to himself by the use of software. These Bitcoin issued by the software will not fall in any of the three permitted categories of pre-paid payment instruments in India: Closed system payment instruments, Semi-closed system payment instruments and Open system payment instruments.[118]

The maximum value of these pre-paid payment instruments cannot exceed INR 50,000 with a minimum validity of six months from the date of activation or issuance to the holder.[119] Banks that comply with the eligibility criteria are authorized to issue three kinds of pre-paid payment instruments and Non-Banking Financial Companies ("**NBFC**") and other persons have been authorized to issue only semi-closed system payment instruments. This infers that the issuer of a pre-payment instrument needs to be either a bank, NBFC or a 'person'. Therefore Bitcoin issued by the software cannot be classified as pre-paid instruments since a server or software cannot be termed as a 'person'.[120]

The software further cannot be regulated within the minimum capital adequacy requirements set for issuers of pre-paid instruments as issuers require a capital of Rs.100 lakh and specific sanction from the RBI.[121] Additionally, only banks which have been permitted to provide Mobile Banking Transactions by RBI are permitted to launch mobile based pre-paid payment instruments (m-wallet and m-accounts).[122] Thereby rendering Bitcoin issued by a mobile-app outside the purview of regulation of pre-paid instruments as these Bitcoin are not circulated by a bank that has prior approval of the RBI. In conclusion, Bitcoin do not fall within the recognized definition of pre-paid instruments.

IX. Applicability of SCRA

The SCRA regulates transactions relating to and involving securities. Section 2(h) of the SCRA defines "securities" to include:

i. shares, scrips, stocks, bonds, debentures, debenture stock or other marketable securities of a like nature in or of any incorporated company or other body corporate;

   a. derivative;

   b. units or any other instrument issued by any collective investment scheme to the investors in such schemes;

   c. security receipt as defined in clause (zg) of section 2 of the Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002;

   d. units or any other such instrument issued to the investors under any mutual fund scheme;

ii. Government securities

iii. such other instruments as may be declared by the Central Government to be securities;

iv. rights or interest in securities

The first issue in this regard is that while all of the above instruments have an underlying capital asset (the assets of the company issuing them for example and hence the reference to the term "**security**"), there is no underlying asset in relation to Bitcoin. The second issue is that Bitcoin are not "issued" by anybody but are created from the activity of mining.

The above aspects also apply in relation to whether Bitcoin could qualify as "derivatives". Section 2(ac) of the SCRA defines a derivative as:

i. security derived from a debt instrument, share, loan, whether secured or unsecured, risk instrument or contract for differences or any other form of security; or

ii. contract which derives its value from the prices, or index of prices, of underlying securities. Since Bitcoin do not fulfil any of the above criteria, they may not qualify as a security (or a derivative) from an Indian law perspective.

The same criteria (related to an underlying security / asset) applies to a derivative as well. Accordingly, Bitcoin cannot be categorized as "derivatives".

X. Bitcoin – Contracts and Enforceability

S. 23 of the Contract Act provides that certain considerations are unlawful and certain contracts may be opposed to public policy. Public policy has not been defined in the Contract Act and is an

118. *See*, http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1902

119. Section 3(42) of the General Clauses Act, 1897; "3(42) "person" shall include any company or association or body of individuals, whether incorporated or not"."

120. RBI Database, *"Draft Guidelines for issuance and operation of Prepaid Payment Instruments in India*".

121. *See*, http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1902

122. In Re: Special Reference No.1 of 2012 (dt. 27.09.2012), Relying on Premium Granites v. State of TN (1994) 2 SCC 691 and Delhi Science forum v. Union of India (1996) 2 SCC 405

evolving expression. The Supreme Court has held that courts ought not to be quick to expand on the scope of what is public policy, they may, in the context of facts and circumstances take into account new developments and explain the same in the context of public policy.

Section 23 of the Contract Act provides:

What consideration and objects are lawful, and what not

The consideration or object of an agreement is lawful, unless - it is forbidden by law; or is of such nature that, if permitted it would defeat the provisions of any law or is fraudulent; of involves or implies, injury to the person or property of another; or the Court regards it as immoral, or opposed to public policy. In each of these cases, the consideration or object of an agreement is said to be unlawful. Every agreement of which the object or consideration is unlawful is void.

The Supreme Court has held that courts would not arbiter on soundness or otherwise of general policy decisions. Further, courts ought not to engage in the exercise of whether one particular policy is good over the other.[123]

There is nothing in law to suggest that Bitcoin are opposed to public policy or otherwise unlawful. A contract relating to Bitcoin, prima facie, is not such that its enforceability would defeat the provisions of law or is otherwise fraudulent. Therefore, a contract respecting Bitcoin, whether it is in relation to mining of Bitcoin, transfer of Bitcoin or transfer of Bitcoin for consideration, is not per se illegal.

An interesting issue that arises is the implications of a contract that provides Bitcoin as consideration, i.e., payment, under the contract. Contract Act does not provide the form or manner in which consideration may be paid by one party to another party. However, in a contract for sale of goods under the Sale of Goods Act, consideration cannot be in kind. As held by the Supreme Court in *Commissioner of Income Tax, Hyderabad v. Motors and General Stores (P.) Ltd.*[124], Section 2(10) of the Sale of Goods Act defines "price" as meaning the money consideration for a sale of goods. The presence of money consideration is therefore an essential element in a transaction of sale under the Sales of Goods Act and not a transaction under Contract Act. If the consideration is not money but some other valuable consideration it may be an exchange or barter but not a sale.

As long as Bitcoin are not currency / legal tender, they can only be considered as 'value for money' or goods. Therefore, Bitcoin would qualify as a consideration under the Contract Act but not as consideration under the Sale of Goods Act.

123. AIR 1968 SC 200

124. *See*, http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247

6. Regulatory Concerns Regarding Bitcoin

There is a growing need for adoption of a concrete regulatory policy regarding cryptocurrencies like Bitcoin in India. So far, the RBI has adopted a hands-off but cautious approach towards the regulation of Bitcoin. RBI on December 24, 2013, issued a press release cautioning users, holders and traders of virtual currencies (VCs), including Bitcoin, about the potential financial, operational, legal, security related risks that they are exposing themselves to.[125] RBI mentioned that it has been looking at the developments relating to certain electronic records claiming to be "Decentralized Digital Currency" or "Virtual Currency", such as, Bitcoin, litecoins, bbqcoins, and dogecoins etc., their usage or trading in the country and the various media reports in this regard. The creation, trading or usage of VCs including Bitcoin, as a medium for payment is not recognized by the central bank or any monetary authority. No regulatory approvals, registration or authorization is stated to have been obtained by the entities carrying on such activities.[126] RBI in its press release also laid down several risks which included:

- VCs being in digital form are stored in digital/ electronic media that are called electronic wallets. Therefore, they are prone to losses arising out of hacking, loss of password, compromise of access credentials, malware attack etc. Since they are not created by or traded through any authorized central registry or agency, the loss of the e-wallet could result in the permanent loss of the VCs held in them.
- Payments by VCs, such as Bitcoin, take place on a peer-to-peer basis without an authorized central agency which regulates such payments. As such, there is no established framework for recourse to customer problems / disputes / charge backs etc.
- There is no underlying or backing of any asset for VCs. As such, their value seems to be a matter of speculation. Huge volatility in the value of VCs has been noticed in the recent past. Thus, the users are exposed to potential losses on account of such volatility in value.
- It is reported that VCs, such as Bitcoin, are being traded on exchange platforms set up in various jurisdictions whose legal status is also unclear. Hence, the traders of VCs on such platforms are exposed to legal as well as financial risks.
- There have been several media reports of the usage of VCs, including Bitcoin, for illicit and illegal activities in several jurisdictions. The absence of information of counterparties in such peer-to-peer anonymous/ pseudonymous systems could subject the users to unintentional breaches of anti-money laundering and combating the financing of terrorism (AML/CFT) laws.

A similar approach was taken by People's Bank of China that ordered financial institutions not to provide Bitcoin-related services and cautioned against its potential use in money-laundering.[127] Following the RBI's notice and similar actions carried out in foreign markets, India's biggest Bitcoin Trading Platform "BuysellBitCo.com" closed its platform amidst growing concern surrounding the trading in digital currencies.[128]

I. KYC Norms – Applicability to Bitcoin

In India, KYC Norms are the norms set by the RBI that require banks to continuously monitor their customers' transactions, keep an up-to-date record of their identity, and take steps simply in case any of the transactions of a customer break from his or her usual pattern of behavior.[129] As already discussed above, the system of Bitcoin uses the block chain technology which allows the system to keep a proper track of the transactions being made. Due to its lack of physical presence, bringing Bitcoin under the current Indian laws can be difficult. The KYC requirements are also being followed by some Bitcoin exchanges before allowing customers to open accounts with them.[130]

Section 3 of the Prevention of Money Laundering Act, 2002 ("**PMLA**") will lose its purpose if the authorities

125. RBI Press Release, "RBI cautions users of Virtual Currencies against Risks", 24 December 2013.Available at: http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247

126. Gerry Mullany, "China Restricts Banks' Use of Bitcoin," The New York Times, (December 5, 2013). Available at: http://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from usingBitcoin.html.

127. Agence France, "India's biggest Bitcoin trading platform halts trade after RBI warning", 28 December 2013.

128. *RBI, Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/ Obligation of banks under PMLA, 2002*, RBI/2013-14/94, available at: http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=8179.

129. https://Bitcointalk.org/index.php?topic=454795.0

130. Section 12 of the Prevention of Money Laundering Act, 2002

are not able to identify the person, making the investigation involving money laundering much more difficult. Financial Institutions, banks and intermediaries are mandated to collect information of the clients.[131] However, it would appear that certain aspects of transactions in Bitcoin cannot be adequately regulated under the existing legal and regulatory framework.

Ultimately, both financial institutions[132] and Intermediaries[133] are poles apart from what the Bitcoin system is. With the advent of Bitcoin the idea that a person or entity handles financial instrument has changed. The question to be answered is, whether the KYC norms as prescribed today are capable of regulating such a system. Even in the event when such norms are applied strictly, there will be others who can, by simply working with the software, mine more Bitcoin.

II. Cross border transfer of Bitcoin

FEMA regulates all inbound and outbound foreign exchange related transactions, in effect regulating (or managing) the capital flows coming into and moving out of the country. Section 3 of FEMA states that other than as provided (and specifically enunciated) in either FEMA (or its underlying rules and regulations) or unless special or general permission of RBI has been obtained, no person shall:

'deal in or transfer any foreign exchange or foreign security to any person not being an authorized person ;[134]

i. make any payment to or for the credit of any person resident outside India in any manner;

ii. receive otherwise through an authorized person, any payment by order or on behalf of any person resident outside India in any manner; and

iii. enter into any financial transaction in India as consideration for or in association with acquisition or creation or transfer of a right to acquire, any asset outside India by any person.'

From the above, it could be argued that purchasing of Bitcoin by a resident Indian from a person resident outside India (where money for purchase of Bitcoin is transmitted through legitimate banking channels) will not be in violation of FEMA. Further, Bitcoin transaction between two residents should also not trigger FEMA and should not therefore be in violation of the same. However, the sale of Bitcoin to a non-resident person (i.e. to a person outside India) by a resident Indian will be in violation of the provisions of FEMA. Further, it can also be regulated by RBI in this condition.

III. Taxation of Bitcoin

In India, taxes are levied either by the central and the state governments. Article 246 of the Indian Constitution confers powers related to legislation of tax rules to state as well as central legislatures. Schedule VII enumerates these subject matters in 3 separate lists.[135] Taxes may be on income or expenditure. When taxation is on income, it may be on Bitcoin representing such income or on Bitcoin representing asset value. Additionally, it may also be on expenditure – cost of acquiring Bitcoin, such as Central Sales Tax, Value-Added Tax or Service Tax. For the purpose of taxation, three possible scenarios emerge:

i. mining of Bitcoin (similar to self-generated goodwill),

ii. transfer of Bitcoin (where Bitcoin are either a capital asset or a stock-in-trade depending on the activity undertaken by the tax payer), and,

iii. transfer of Bitcoin as consideration (where Bitcoin are either a capital asset or a stock-in-trade depending on the activity undertaken by the tax payer).

131. Section 45 IA of Reserve Bank of India Act, 1934

132. See SECURITIES AND EXCHANGE BOARD OF INDIA (INTERMEDIARIES) REGULATIONS, 2008 (g) "intermediary" means a person mentioned in clauses (b) and (ba) of sub-section (2) of section 11 and sub-section (1) and (1A) of section 12 of the Act and includes an asset management company in relation to the Securities and Exchange Board of India (Mutual Funds) Regulations, 1996, a clearing member of a clearing corporation or clearing house and a trading member of a derivative segment of a stock exchange but does not include foreign institutional investor, foreign venture capital investor, mutual fund, collective investment scheme and venture capital fund.

133. An authorized person is defined as an authorized dealer, money changer, offshore banking unit or any other person for the time being authorized under sub-section (1) of section 10 to deal in foreign exchange or foreign securities.

134. Article 246 of the India Constitution,

135. Section 2 (7) of the Income Tax Act, 1961.

IV. Income Tax

Taxation of income in India is governed by the provisions of the Income Tax Act, 1961 (“**ITA**”). Under the ITA, residents are subject to tax in India on their worldwide income, whereas non-residents are taxed only on income sourced in India. However, non-residents, who are resident of a country with which India has signed a tax treaty, have the option of being taxed as per the tax treaty or the ITA whichever is more beneficial. Every person, who is an assessee[136] and whose total income exceeds the maximum exemption limit, should be chargeable to the income tax at the rates prescribed.

Bitcoin may be considered to be currency or a capital asset. However, this is not yet clear under Indian law which makes it difficult to conclude how it may be taxed. The following discussion considers the tax implications on Bitcoin related transactions under the Indian Income tax law.

V. Currency

Although for the purpose of general regulatory and commercial laws, Bitcoin may not be treated as currency, the income tax authorities may still treat Bitcoin as currency for the purpose of taxation. In such a case, Bitcoin are to be treated as consideration and the tax implication is not on Bitcoin but the transaction itself. For instance, if the seller is a regular trader, the income should be considered as business income at the rate of 30%. If not business income, such income would be in the nature of capital gain.

Under Indian law when a capital asset is transferred, the profit/gain that arises out of such transfer is taxable as income.[137] The tax liability, when such a transfer is made, is calculated by deducting the cost of acquisition of the capital asset from the sale proceeds and applying the tax rate to the difference.[138] According to the Supreme Court, it is required that the income be both “computable as well as chargeable” under the provisions of the ITA for capital gains to be taxable in India.[139] A study of recent case laws reveals that it has been held consistently by the Indian courts that the “computation” machinery as provided under the ITA is inextricably linked with the chargeability of tax on capital gains. It has also been held that, if in a particular case, the computation provisions cannot be applied, it is suggestive of the fact that it was not in the contemplation of the charging section and consequently, when the computation provision fails, no tax can be levied.[137]

An amendment was made to the ITA to specify that in relation to a trade mark or brand name associated with a business or a right to manufacture, produce or process any article or thing, the cost of acquisition should be considered to be the following:

i. the amount of the purchase price in the case of acquisition of such asset by way of purchase from a previous owner; and

ii. nil in all other cases.[140]

Hence, the entire sale proceeds will attract capital gains tax levy, where the cost of acquisition is nil.

Bitcoin however is not covered by this exception. Thus, there might be some instances where the taxpayer could enjoy tax-free income. But in cases where the Bitcoin have been mined, it is possible that authorities will treat income of sale as taxable business income, even though it might be difficult to determine the cost.

136. See, http://business.gov.in/taxation/capital_gains.php

137. See,http://www.incometaxindiapr.gov.in/incometaxindiacr/contents/tpi/Unedited%20How%20to%20compute%20your%20capital%20gains%20 2008-09.pdf

138. CIT v. B.C. SrinivasaSetty, (1981) 128 ITR 294 (SC).

139. Except those acquired through inheritance, gift, will, partition etc. (situations are not relevant here).

140. http://www.incometaxindiapr.gov.in/incometaxindiacr/contents/tpi/Unedited%20How%20to%20compute%20your%20capital%20gains%20 2008-09.pdf

Mining of Bitcoin	Transfer of Bitcoin	Transfer as consideration
Mining should not be considered as an activity which is taxable. Considering that Bitcoin is not covered by the exception as provided above, mining should not be taxed as capital gains or business income under the ITA. However, it is possible that tax authorities will treat the income that arises on sale as taxable business income, even though it might be difficult to determine the cost	Bitcoin may either be capital asset or stock-in-trade. Since Bitcoin is not covered by the exception, there might be some instances where the taxpayer could enjoy tax-free capital gains which arise on transfer of Bitcoin. Ordinarily, there are no such exceptions in respect of income that arises on transfer of Bitcoin as stock-in-trade. However, deductions are permitted may be claimed on income that arises from transfer of Bitcoin as stock-in-trade.	In this case, Bitcoin represents consideration for the asset transferred / service provided and is treated as if it is currency. The transaction will be subject to tax depending on whether the underlying asset is a capital asset or stock-in-trade. However the Bitcoin ***itself*** cannot be taxed since the Bitcoin, in this case, represent 'currency' and the transaction has already beensubjected to taxation (either as business income or capital gains).
	Gains on transfer of Bitcoin as capital assets are taxed under the following two heads: *i. Long-term capital gain:* When the property is held for more than 36 months, the gains are taxed as long-term capital gains. *ii. Short-term capital gains:* Cases in which the capital asset is held for less than 36 months the gains will be taxed as short-term capital gains.	

VI. Central Sales Tax / Value Added Tax

The Central Sales Tax Act, 1930 ("**CST Act**") provides for the levy, collection and distribution of taxes on sales of goods in the course of inter-state trade. For a Bitcoin transaction to be taxed under the CST Act, there should be a sale – i.e., transfer of property and transfer of goods.

"Sale" is defined under Section 2(g) of the CST Act, as follows:

> *"sale", with its grammatical variations and cognate expressions, means any transfer of property in goods by one person to another for cash or deferred payment or for any other valuable consideration, and includes,–*
>
> *i. a transfer, otherwise than in pursuance of a contract, of property in any goods for cash, deferred payment or other valuable consideration;*
>
> *ii. a transfer of property in goods (whether as goods or in some other form) involved in the execution of a works contract;"*

The essentials that need to be fulfilled by a transaction to be categorized as sale are:

i. Transfer of property by one person to another in goods

ii. Payment in the form of cash, deferred payments or any other valuable consideration.

Where Bitcoin is exchanged for currency or any other consideration, the above essentials of sale should be satisfied. However, it also needs to be established whether Bitcoin can be considered as 'goods' under the CST Act. Goods under CST act are defined as:

> *"goods" includes all materials, articles, commodities and all other kinds of movable property, but does not include newspapers, actionable claims, stocks, shares and securities;"*

As already discussed in the previous sections, Bitcoin may fall under the category of commodity and thus come under the definition of goods under the CST Act and thus fulfilling the essentials of a transaction of sale.

Similarly, Section 6 of the Maharashtra VAT Act 2002 ("**MVAT Act**") provides that tax should be levied on goods mentioned in Schedule B, C, D and E of the

MVAT Act. Schedule C, entry 39 includes goods of "intangible or incorporeal nature" as notified from time to time by the State Government in the Official Gazette. The State Government pursuant to the above sections has issued notifications to classify various kinds of intellectual property including patents, trademarks, copyright etc. as goods.[141]

However, MVAT Act clearly states that for a property to be considered as "goods" for tax purposes, it should be notified by the Government. Virtual currencies like Bitcoin have not been notified are hence should not be liable to be taxed as goods under the abovementioned provisions and consequently, transfer of Bitcoin cannot be taxed under MVAT Act.

In another situation, where Bitcoin are exchanged for goods, Bitcoin can be considered as "consideration in kind". The definition of sale under the CST Act, as stated above, provides that a sale is said to have been made when any transfer of goods takes place for cash, deferred payment or "other valuable consideration". However, the issue that needs to be considered is whether Bitcoin can be considered as "other valuable consideration". Courts have, on many occasions delved into the meaning of this phrase.[142] The Supreme Court in the case of *Devi Das Gopal Krishna and Others v. State of Punjab* [143] while interpreting the same phrase in the Punjab General Sales Tax Act has opined:

"Expression "valuable consideration" in the definition of "sale" takes colour from the preceding expression "cash or deferred payment" and therefore the consideration for sale can only mean some other monetary payment in the nature of cash or deferred payment and would not comprehend a transaction in the nature of barter."

Hence, the coverage provided by this definition is to be ascertained on case to case basis since there is no straight jacket formula to know what will constitute as "valuable consideration".

VII. Service Tax

Service tax is levied by the central government at 12.36% on all services provided in India except certain specified services. Service providers can take credit for service tax paid on input services utilized and for excise duty paid on inputs and capital goods (barring certain specified inputs). Services provided outside India are not subject to service tax in India. Typically, services are considered to be provided in India if the service recipient is located in India (even though the services may actually be provided outside India), except when specifically provided otherwise.[144] In case of online information and database access or retrieval services, it has been specifically provided that the services would be construed to be provided at the location of the service provider.

The 2015 Budget proposes to increase the rate of service tax to from 12.36% (inclusive of cesses) to 14%.

For service tax to apply, Bitcoin needs to fall under the category of "taxable service" (charging section). "Taxable Service" is defined in Section 65(105) of the Chapter V of the Finance Tax Act, 1994. Here it may fall under Clause (zh) which states that taxable service includes services to any person, by [any person], in relation to on-line information and database access or retrieval or both in electronic form through computer network, in any manner; or Clause (zzze) stating "to its members, [or any other person], by any club or association in relation to provision of services, facilities or advantages for a subscription or any other amount".

Therefore, the act of mining may be considered as a taxable service in terms of the clauses under the Finance Act as stated above.

Transfer of Bitcoin itself may not attract service tax since service tax is leviable on provision of services and not transfer of goods. Unless there is a service which is provided in relation to transfer of Bitcoin or mining of Bitcoin, service tax may not be levied on Bitcoin related transactions. However, Section 67 (1) (iii) contemplates receipt of consideration in kind or in some other manner which is not 'ascertainable' and consequently, merely because consideration has been made in the form of Bitcoin the transaction will not be exempted from service tax.

141. Notification No. No. VAT-1505/CR-114/Taxation-1

142. Vijaya Aluminium Industries Vs. State of Andhra Pradesh (1996) 103 STC 508

143. (1967) 20 STC 430 (S.C.)

144. Place of Provision of Services Rules, 2012

7. Intellectual Property Issues

Traditionally, inventions, literary works, artistic works, designs and trademarks formed the subject matter of intellectual property law protection. However, with the advent of new technologies coupled with the advancements in the digital space, various forms of intellectual property rights are evolving. The challenge for a business would be in identifying best methods for protection of its intellectual assets. With the development of virtual currencies (including Bitcoins) and other modes of online payment systems, we examine some of the key intellectual property rights available.

I. Trademark

To trace the history of the origin of the term, the word 'Bitcoin' first appeared in Satoshi Nakamoto's white paper explaining the details of the Bitcoin software.[145] As of date, MtGox, the world's most prominent Bitcoin exchange based in Tokyo, currently holds the trademark for 'Bitcoin'.[146]

As per Indian trademark law, a trademark protection can be accorded to a mark [147] which is capable of being represented graphically and which is capable of distinguishing the goods or services of one person from those of others.[148] Thus, the word 'Bitcoin' and any logos [149] connected with Bitcoins could acquire trademark protection in India under this law. However, a question that arises is whether the term "Bitcoin" should be accorded trademark protection in the first place. Since the term "Bitcoin" is widely used by the public in a generic manner, without association or reference to a particular entity providing an online Bitcoin payment system or other Bitcoin related financial services, it may be difficult for anyone to prove distinctiveness and uniqueness of the Bitcoin mark at the time of seeking registration of the mark.

In India, there are trademark applications filed by Bitcoin traders for registration of various word marks that include the term "Bitcoin" within them. These applications are currently pending registration before the Indian Trade Marks Registry ("**TMR**"). Specifically, there is also an application pending before the TMR for registration of the word mark "Bitcoin" made by URS Wafler.[150]Trademark protection for the word marks that include the term "Bitcoin", and various Bitcoin logos is essential for financial institutions dealing in Bitcoin transactions and online payment systems. However, if several entities use similar word or logo marks, it is likely to confuse the members of public regarding the various Bitcoin platforms / Bitcoin exchanges represented with various visually or phonetically similar Bitcoin marks.

II. Patent

In India, a patent may be registered for an invention that is novel, non-obvious and has utility. While Bitcoins are "mined" by individuals using software and specialized hardware and result in creation of complex algorithms, the process of mining Bitcoins may not qualify for patent protection in India, especially if the techniques and processes are available in the public domain. Further, under Indian patent law, a mathematical or business method or a computer program per se or algorithms are not inventions[151] and are hence not patentable in India. In addition, it may be also difficult to establish novelty for Bitcoin related algorithms and computer programs for the purpose of terming them as 'inventions'.

III. Copyright

As described above, Bitcoin is a software-based system which was introduced as open-source software in 2009[152] Under the Indian Copyright Act, 1957, a computer program is protected as literary work. Section 2 (ffc) of the Copyright Act, 1957 defines a 'computer program' as a "set of instructions expressed in words, codes, schemes or in any other

145. Bitcoin: A Peer-to-Peer Electronic Cash System Available at: https://bitcoin.org/bitcoin.pdf Last accessed: January 30, 2015.

146. Mt. Gox to Sell Bitcoin Trademark, But Could a Buyer Enforce It? Available at: http://www.coindesk.com/mt-gox-sell-bitcoin-trademark-buyer-enforce/ Last accessed: January 30, 2015.

147. Section 2 (m) of the Trade Marks Act, 1999 defines mark to include a "device, brand, heading, label, ticket, name, signature, word, letter, numeral, shape of goods, packaging or combination of colours or any combination thereof."

148. Section 2(zb) of the Trade Marks Act, 1999

149. One of the most popularly used Bitcoin logos / symbols may be viewed at: http://bitcoinsymbol.org/. Last accessed: February 2, 2015.

150. Trademark Application Number 2638963

151. Section 3(k) of the Patents Act, 1970.

152. *Supra* note 23.

form, including a machine readable medium, capable of causing a computer to perform a particular task or achieve a particular result."

The program in the underlying platform used in the generation and trading of Bitcoins or the programs which run in the back end of the Bitcoin exchange and facilitate trading, would constitute a 'computer program'. However, the Bitcoin protocol and software are published openly and any developer around the world can review the code or make their own modified version of the Bitcoin software.[153] No exclusivity is generally claimed in open source software. Since developers can review the code and make their own modified version of the Bitcoin software[154], each revision may give rise to a new copyright and thus it will be difficult to ascertain who holds the copyright in the codes. In the mining process, new Bitcoins are generated and introduced into the system, thus possibly leading to the creation of new codes, schemes or other components of the computer program, which may be entitled to copyrighted protection. Such an issue may arise with respect to who may be the author of such new works created. However, there does not appear to be any commercial value in the codes. Hence, the issue appears to be more of academic nature.

153. https://bitcoin.org/en/faq. Last accessed: February 5, 2015
154. https://bitcoin.org/en/faq Last accessed: February 5, 2015

8. Security Issues

One of the most important issues in the digital space and use of virtual currency is security. Bitcoin exchanges and other financial institutions dealing in Bitcoin transactions have been prone to security threats and hacks in the recent past; one instance being early in 2014 when hackers reportedly stole more than USD 5 million in virtual currency from Bitstamp, a major Bitcoin exchange.[155] In early 2014, Mt. Gox announced that it lost Bitcoins of value equivalent to USD 620 million of which a major portion belonged to its customers at the time.[156]

In the Indian context, the Information Technology Act, 2000 ("**IT Act**") contains certain provisions which may be relevant to examine from a security perspective when discussing Bitcoins. The IT Act deals with various offences such as hacking and tampering with computer source documents which may be relevant when discussing security issues relating to Bitcoins.

The IT Act defines a 'computer' as *"any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network."*[157]

Since Bitcoins (i) area virtual software-based crypto-currency, (ii) are transacted through online payment systems, platforms and portals, (ii) there is an underlying software used in such systems, platforms and portals, it is quite likely that Bitcoins would fall within the ambit of a 'computer'.

If Bitcoins are considered to fall within the ambit of 'computers' as defined in the IT Act, it would be prudent to analyze various provisions of the IT Act relating to computer-related offences, some of which are criminal in nature.

I. Hacking

Section 43 of the IT Act provides that any person, without the permission of the owner or any person in charge of a computer, computer system or computer network:

i. accesses or secures access to such computer, computer system or computer network;

ii. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

iii. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

iv. damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

v. disrupts or causes disruption of any computer, computer system or computer network;

vi. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

vii. provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

viii. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, shall be liable to pay damages by way of compensation to the person affected by such acts.

II. Hacking with Criminal Intention

Section 66 of the IT Act states that if any of the

155. *Hackers steal $5 million from major bitcoin exchange;* Available at: http://fortune.com/2015/01/05/bitstamp-bitcoin-freeze-hack/ Last accessed: January 29, 2015.

156. *The Troubling Holes in MtGox's Account of How It Lost $600 Million in Bitcoins; Available* at: http://www.technologyreview.com/view/526161/the-troubling-holes-in-mtgoxs-account-of-how-it-lost-600-million-in-bitcoins/ Last accessed: January 29, 2015.

157. Section 2(i), IT Act

abovementioned acts as enlisted under Section 43 are performed dishonestly[158] or fraudulently,[159] such person performing such acts shall be punishable with imprisonment for a term of up to 3 years or with a fine of up to INR 5,00,000, or both.

III. Identity Theft

- Section 66C of The IT Act provides for a punishment of imprisonment of a term of up to 3 years and a fine of up to INR 1,00,000 in case of offences relating to identity theft, i.e., where a person fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person.
- Section 66D of The IT Act provides for a punishment of imprisonment of a term of up to 3 years and a fine of up to INR 1,00,000 in case of offences relating to cheating by impersonation by using a computer resource.

Although the general perception is that the making of false entries by any person is almost impossible and that the use of pseudonyms in dealing with Bitcoins is a generally safe practice, given technological advances, there could be some scope of impersonation or identity theft.

IV. Cyber Terrorism

Section 66 F(1) of The IT Act provides a punishment of imprisonment which may extend to imprisonment for life, for acts of cyber terrorism. Section 66F of the IT Act provides that whoever,

"(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-

i. denying or cause the denial of access to any person authorized to access computer resource; or

ii. attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

iii. introducing or causing to introduce any computer contaminant; and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.[160]

Acts of security breaches and hacking may constitute damage or destruction to property and in exceptional cases, such unauthorized access to data may pose a threat to the security of the State or foreign relations. Such acts may be construed as acts of cyber terrorism if there is an intention to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people. However, in the present scenario, due to the limited use and extent of Bitcoin transactions in India, it is unlikely that such acts would affect the unity, integrity, security or sovereignty of India or cause terror among people. If, however, Bitcoin exchanges and the use of Bitcoins were as wide spread as the securities market, then if such security breaches were initiated in the securities market, such actions may be construed as acts of cyber terrorism due to the widespread extent and high value of securities held by numerous people and, as such acts would cause rippling adverse effects in the Indian economy and derail public order, as well as the sovereignty and security of the nation.

158. Section 24 of the Indian Penal Code ("IPC") defines "dishonestly" "*as whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly"*."

159. Section 25 of the IPC defines "fraudulently" as *"a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise."*

160. Section 66-F(1), IT Act.

9. Privacy and Data Protection

The paper on Bitcoins that was authored by Satoshi Nakamoto[161] acknowledges that since the use of Bitcoins essentially means that all transactions will announced publicly, there may be privacy concerns. This paper addresses privacy concerns by stating the following:

The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were

In India there is no separate legislation dealing with right to privacy. The Supreme Court has recognized the "right to privacy" as a subset of the larger "right to life and personal liberty" under Article 21 of the Constitution of India. However a right under the Constitution can be exercised only against any government action. Non-state initiated violations of privacy may be dealt with under principles of torts such as defamation, trespass and breach of confidence, as applicable. However the law of torts is not very well developed in India. Accordingly there does not appear to be a special legislation dealing with privacy issues in the use of Bitcoins.

Apart from privacy issues, there are issues of data control and protection that may be discussed.

The IT Act[162] accords protection to certain items of sensitive personal data or information ("**SPDI**") which are capable of identifying natural persons and sets out a set of compliances to be undertaken by entities that collect, store or process such SPDI in India or transfer such SPDI to or from India.

It does not seem that the legislature had taken into account Bitcoins (and the impact of the use of peer to peer cryptocurrency) when formulating the data protection rules under the IT Act. Given the legal uncertainty, it may be prudent to discuss whether there is any aspect in the use of Bitcoins which can attract the provisions of the data protection rules under the IT Act.

The definition of SPDI contains a list of personal information which can identify a natural person. From this list, the items of SPDI which are relevant to be considered when discussing Bitcoins are

i. passwords[163] and

ii. financial information such as Bank Account or Credit Card or Debit Card details or other payment instrument details.

- When dealing with Bitcoins, it is possible that different types of passwords (which by its definition include encryption and decryption keys) are collected, stored and processed – thus ostensibly triggering the applicability of the data protection provisions of the IT Act. However, the next question to be addressed is who generates such encryption keys and how are they shared. Given that such encryption keys are randomly created and given that the Bitcoin network is not really controlled by any one entity in any jurisdiction[164] there is a grey area whether the IT Act would apply in such situations.

- It is not entirely clear whether a Bitcoin would be considered to be financial information within the definition of SPDI. The definition contemplates payment instrument details rather than a currency form, which is what a Bitcoin (being a cryptocurrency) is. Further Bitcoins are not associated with any established financial institution (such as the apex bank), a situation which does not seem to have been contemplated by the legislature

161. *Bitcoin: A Peer-to-Peer Electronic Cash System* available at https://bitcoin.org/bitcoin.pdf

162. Read along with *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Information) Rules 2011*

163. The IT Act defines passwords as follows: *Password means a secret word or phrase or code or pass phrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information.*

164. https://bitcoin.org/en/faq#who-controls-the-bitcoin-network

10. Risks Related to Bitcoin

The question of how far adherent users of the Bitcoin currency will derive satisfaction in Bitcoin currency is shrouded with speculations. However, certain factors and recent incidents inform current and potential users of what could unfold in the Bitcoin regime.

I. Cyber Attacks and Hacking: "Virtual Bank Robbery"

Attacks by "cyber thieves" are becoming frequent with the passing of time. Especially the Bitcoin community has been hit by such thefts quite repeatedly. This not only creates panic in the Bitcoin community but also leads to a decline in the value of the currency. Cyber security will be a constant concern, mostly because the transactions are restricted only to the cyber environment.[165]

One of the most discussed examples of such an attack (Distributed Denial-of-service) was targeted at Mt. Gox, one of the largest Bitcoin exchanges. The result of this attack was that the value of Bitcoin went down rapidly.[166] It is suggested by some that these hackers are trying to sustain a loop where "they sell Bitcoin when values are high, then mount an attack that forces prices to crash, buy up the cheaper coins and then let the value climb again".[167] These issues and frequent attacks have majorly contributed in damaging the reputation of Bitcoin by scaring investors who do not want to take the risk of suffering huge losses without any insurance to cushion the blow. Due to lack of confidence in Bitcoin and hence lack of insurance, there is no sign of consumer protection in the Bitcoin community.

II. Price Fluctuation and Inflation

One of the major reasons why today many businesses and merchants avoid using Bitcoin is that it is new and the volatility of Bitcoin value is extremely high.[168] This again leads to the uncertainty and reduced confidence in the currency. Although, some think that in spite of these flaws, one of the most valuable consolations might be that there can be no artificial inflation or deflation of the currency.[169]

III. Fraud

Some say that Bitcoin will keep appealing to charlatans coming up with destructive schemes as explained above since Bitcoin offers benefits of privacy as well as limited oversight by the regulators. When compared with the traditional fiat currency that not only has extensive regulatory oversight but also offers very less privacy, Bitcoin does seem like the better option for the fraudsters.[170] It may also be noted that fraud of this nature in addition to harming the customers personally and decreasing the value of the currency itself, can also lead to severe damage to the economies as well.[171]

IV. Uncertainties in the Government Policies

Since most jurisdictions have not made a decision regarding the status and treatment of Bitcoin in the economy, as already discussed above, the uncertainty is a deal breaker for many new prospective users of Bitcoin. One of the major dangers here is that any government might come around and declare it illegal, leaving the investors without remedy and helpless.

165. Nicholas A. Plassaras, 'Regulating digital currencies: Bringing Bitcoin within the reach of the IMF', Forthcoming, 14 Chi J intl L _ (2013) Pg. 12.

166. BBC News Technology, 'Hack attacks hit Bitcoin exchange rates' <http://www.bbc.co.uk/news/technology-22026961>

167. Ibid.

168. Joshua Davis, Department of Technology 'The Crypto-Currency', The New Yorker (10 October 2011) Pg. 68

169. Nicholas A. Plassaras, 'Regulating digital currencies: Bringing Bitcoin within the reach of the IMF', Forthcoming, 14 Chi J intl L _ (2013) Pg. 8.

170. US Securities and Exchange Commission's Office of Investor Education and Advocacy, 'Investor Alert (Ponzi Schemes Using Virtual currencies "http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf" accessed 07/01/2015.

171. See, http://uk.reuters.com/article/2014/09/11/uk-britain-boe-Bitcoin-idUKKBN0H61HL20140911

11. Vulnerabilities in Bitcoin Transactions

This arena of virtual transitions is relatively novel and largely untested. This means that, just like any new technology or innovation there is a high possibility that many loopholes might exist in this system that have not been detected yet. This only adds to the appeal of the Bitcoin for financial criminals. Most prominent of these offences which are already existent in the traditional financial world and which may extend to Bitcoin are money laundering and terrorist financing.

I. Money Laundering

One of the major enabling factors for money laundering is lack of uniform financial jurisdiction across the globe. This is the reason why certain areas are labelled as "tax havens". It may be noted that money laundering contributes largely to the deteriorating state of economies in the world. In most matters, the funds that are being laundered are earnings through corruption and bribery, which needless to say are rampant in under-developed and developing nations. There is sharp contrast between the effects of money laundering on developed and developing nations. By utilizing these funds for economic stability, it supports the economic development of developed countries. On the other hand, developing nations due to being cash starved, face stagnated political and economic growth.[172] Hence, this could be a serious threat to India.

II. Drug Trafficking

Silk Road, launched in June 2011, and only reachable by people using Tor, the software that lets one surf the dark web anonymously. Silk Road was used by countless people to get access to illegal merchandise, spanning from drugs to assassins for hire. An estimate of $1.9 million dollars' worth of Bitcoin transactions per month were done according to a research.[173] This came as a confirmation of the fact that Bitcoin is fast becoming the first choice for drug dealers to shelter themselves from the scrutiny of the law.

III. Tax Avoidance and Evasion

There are very few nations who have released rules or guidelines regarding the treatment of Bitcoin for the purpose of taxation. While most countries have not resolved the issue of taxation of Bitcoins and transactions in relation to Bitcoins, it is speculated that the answer might be in affirmative.[174] However, in case other countries follow suit and bring Bitcoin under tax laws, it must be kept in mind that since it is not a government backed currency, people might not report all transactions made when Bitcoin is appreciated. This will make it even more difficult for the government to detect and curb tax evasion.[175]

IV. Blackmailing

Mitt Romney, the Republican presidential candidate in 2012 was blackmailed by a man who claimed to have gained access to his tax record through PwC network. He threatened to reveal the information to the public if a payment of $1 million worth of Bitcoins was not made to him. The incentive in this case seems to be the anonymity that Bitcoin transaction affords to the parties.

V. Terrorist Financing

The concepts of terrorist financing and money laundering have been distinguished by the International Compliance Association. Terrorist Financing is concealment of future application of financial resources that may be illegal wherein such resources are obtained from a legitimate source. On the other hand Money laundering refers to a past or present benefit.[176] Traditionally terrorism has been defined as the use of threat or violence to achieve a political end. However, this definition is stale. Many jurisdictions are now making an effort to overhaul the definition to keep it viable in today's world. For example, under the Terrorism Act 2000, it has been defined as follows:

"the use or threat of action which:

172. Nikolei M Kaplanov, 'Nerdy money: Bitcoin, the private digital currency, and the case against its regulation' (2012) 25 Loy. Consumer L. Rev. 111, 121.

173. The Economist, 'Monetarists Anonymous; Bitcoin' The Economist (London, Sept 29, 2012) Vol 404, Issue 8804, Pg. 80.

174. Crypto-Currency Legal Advocacy Group, Inc., 'Staying Between the Lines: A Survey of U.S Income Taxation and its Ramifications on Crypto-Currencies' Available at http://theclag.org/CM%231001Final.pdf.

175. Thomas S. GrothEsq, 'Tax implications of Bitcoin (and traditional alternative currencies)' Available at http://www.irsmedic.com/2013/04/05/can-you-be-taxed-for-spending-Bitcoin/

176. International Compliance Association 2013 Workshop Note on Anti Money Laundering Awareness, Pg. 38.

i. is designed to influence the government or an international government organization or to intimidate the public or a section of the public;

ii. involves serious violence against a person;

iii. involves serious damage to property;

iv. endangers a person's life other than the person committing the action;

v. creates a serious risk to the health or safety of the public or a section of the public."[177]

Undeniably, the counter-terrorist financing measures could easily be evaded by using Bitcoin owing to its virtual nature. If the legislations on counter terrorism and other forms of laundering issues are not amended to cover digital currencies as Bitcoin, the problem could very much worsen. The Joint Money laundering Steering Group (JMLSG) Board approved a revision to guidance with regard to Electronic Money. In addition, the Financial Action Task Force (FATF) recognized that the crypto and digital currency pose very real threats and recommended among other things that countries should identify and assess the terrorist financing risks that may arise in relation to use of new or developing technologies.

It is widely known that today owing to the popularity of the currency; donations by many groups, legitimate and illicit alike are being accepted in the form of Bitcoin.[178] For example the responsibility for break in, in one of the Sony (SME) websites was claimed by a group called LulzSec, who also confirmed that they had received over $18,000 worth of Bitcoin in the form of donations. Also, as already mentioned, Wikileaks, Mint, Dell etc. also accepted donations in the form of Bitcoin. It is pertinent to note that, the volume of the amounts donated to illicit groups is immaterial, since to the people seeking to finance terrorism anonymously, Bitcoin might come in handy as not many formalities and account information is require to complete the transaction as opposed to the traditional fiat currencies.

177. Toby Graham, Evan Bell, Nicholas Elliot, Money Laundering (1st Edition, Reed Elsevier (UK) Ltd 2003) Pg. 56-57. See also, Terrorism Act 2000, s.1.

178. http://www.Bitcoinvalues.net/who-accepts-Bitcoin-payment-companies-stores-take-Bitcoin.html

12. Setting up Bitcoin Related Business in India

It must be noted that in order to carry out any business in India, a foreign person has to either operate through a branch, or through a subsidiary in India. An Indian person may choose to operate either individually (as a sole proprietor), through a firm (such as a partnership) or a body corporate (such as a company or a limited liability partnership). There are other mechanisms for operating a business as well, but the above mentioned are the most common.

Broadly speaking, in order to commence business in India, various structures/ entities (incorporated and unincorporated) may be adopted. A brief overview of the different entities is provided below.

Incorporated entities in India are governed by the provisions of the Companies Act, 2013 and the rules thereunder (“**Act**”). As per the Act, two kinds of entities may be established: (i) private limited company; and (ii) public limited company. Some of the key characteristics of a private limited company are as follows: (i) minimum paid-up capital of INR 100,000; (ii) number of shareholders must be a minimum of 2 and maximum of 200; (iii) transferability of shares is restricted; (iv) invitation to the public to subscribe to the securities of the private company is prohibited.

A few distinguishing characteristics of a public limited company are as follows: (i) minimum paid-up capital of INR 500,000; (ii) number of shareholders must be a minimum of 7, with no maximum prescribed; (iii) shares of a public company are freely transferable; (iv) public company may invite the public to subscribe to its securities.

The incorporation process of a private company is faster when compared with that of a public company. Further, private companies provide more flexibility than public companies in conducting operations, including the management of the company and the payment of managerial remuneration. However, since public companies provide for better exit options and allow for inviting the public to subscribe to its securities, public companies may be preferred over private companies depending on the nature of business involved.

Other than when persons operate individually or without association, unincorporated entities in India are primarily of two types: (i) limited liability partnership; and (ii) partnership. A limited liability partnership (“**LLP**”) is a form of business entity which permits individual partners to be shielded from the liabilities created by other partners’ business decisions or misconduct. In India, LLPs are governed by the Limited Liability Partnership Act, 2008. LLP is a body corporate and exists as a legal person separate from its partners.

A partnership, on the other hand, is a relationship created between persons who have agreed to share the profits of a business carried on by all of them, or any of them acting for all of them. A partnership is not a legal entity independent of its partners. The partners own the business assets together and are personally liable for business debts and taxes. In the absence of a partnership agreement, each partner has an equal right to participate in the management and control of the business and the profits / losses are shared equally amongst the partners. Any partner can bind the firm and the firm is liable for all the liabilities incurred by any partner on behalf of the firm.

Various legal, commercial and tax considerations have to be taken into account before zeroing down on the nature of entity to be established.

Bitcoin Blockchain for Distributed Clearing: A Critical Assessment[1]

Robert Sams – Founder and CEO, Clearmatics

Abstract

There has recently been a dramatic increase in interest in the idea of using distributed consensus technology to facilitate the settlement of financial transactions. One strategy that has been advocated attempts to use the Bitcoin blockchain, running meta-protocols on top of that network, so that off-chain assets such as securities and property titles can leverage the same transaction protocol used by the endogenous on-chain cryptocurrency asset. This article explains Bitcoin's unique flavor of distributed consensus algorithm (hash-based proof-of-work) and how it was motivated by a design goal of censorship-resistant digital cash. It then shows that censorship-resistant consensus has no mechanism for enforcing the correspondence between blockchain reality and legal reality that off-chain assets require. It also suggests that the security of the Bitcoin network itself would be compromised by such an attempt.

1 This is an edited version of a blog that originally was published at http://www.clearmatics.com/2015/05/no-bitcoin-is-not-the-future-of-securities-settlement/

BITCOIN BAD, BLOCKCHAIN GOOD?

Bankers can be forgiven for being confused about blockchain technology. For months they've been told that blockchain and other distributed consensus technology can revolutionize the payments, clearing, and settlement infrastructure of the financial system, but that the bitcoin blockchain just won't do. This suits bankers fine, as few were ever anything but dismissive of the world's most popular cryptocurrency.

But then earlier this year, Nasdaq (2015) announced a project that will actually use the bitcoin blockchain to "facilitate the issuance, transfer, and management of private company securities" on their Nasdaq Private Market platform. So, what is going on?

No sooner had the press release circled around the small and sometimes befuddled group of financial types devoted (or at least instructed) to exploring this technology, when IBM's Richard Brown (2015) comes out with the warning to "ignore Bitcoin at your peril." And then this was followed by Chris Skinner's (2015) post, which suggests that the bankers' confusion is really just a case of the financiers having never understood the inner workings of bitcoin in the first place:

> "So why would someone as intelligent and informed as Reid Hoffman – and Marc Andreessen, Richard Branson, Wence Cesares, Jon Matonis, et al – be so pro-bitcoin when the banks are not. My answer is that most of the people dissing bitcoin haven't looked under the hood.
>
> So here are two test questions for all of you reading this and thinking Bitcoin Bad, Blockchain Good.
>
> One, have you actually read Satoshi Nakamoto's white paper?
> Two, can you explain to me exactly why the blockchain is good?
> I don't do this, as I don't want to embarrass anyone, but I'm guessing that 99% of the Bitcoin Bad, Blockchain Good people would answer no to both questions."

Leaving the provocative aspect aside, he's probably right in that most bankers would answer "no" to his two questions. This might also be true for the majority of bitcoin's most vocal cheerleaders. Skinner then proceeds to the argumentum ad verecundiam and quotes the abstract of Nakamoto's's (2008) famously elegant whitepaper:

> "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers."

This article breaks down this abstract sentence by sentence and gives a non-technical explanation of how bitcoin works and why it's interesting. Then there will be a discussion to explain why the idea of using the bitcoin blockchain for securities settlements is misguided. This is not meant to knock Nasdaq for choosing a bitcoin meta-protocol for their project. It's a good way for them to cut their teeth in this area without devoting much capital expenditure. However, those who think that this news portends a future securities settlement architecture based on the bitcoin blockchain couldn't be more wrong.

A SIMPLE INTRODUCTION TO THE BITCOIN PROTOCOL

The first two sentences of Nakamoto's abstract make clear the design objectives behind bitcoin.

> "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending." [Nakamoto (2008), 1]

It has been known for a long time, mainly because it is rather obvious, that cryptographic signatures and public keys can be chain-linked to form an unforgeable record of transactions for, say, digital cash (or any ledger record for that matter). Crypto proof replaces the notary. Counterfeiting ledger assets is impossible, and theft or misappropriation cannot happen without gaining access to the asset owner's private key [see appendix].

But you still need an authoritative record of these transactions somewhere, such as a database, or else there is no way to prevent someone from spending his or her digital cash more than once (a

"double-spend"). If one party gives as second a crypto-proof that some asset belongs to it and that it has been sent to the second party, the second party has no way of knowing that the first party hasn't already done that with someone else, unless both parties can refer to a definitive ledger of timestamped and crypto-signed transactions, a ledger maintained as a database hosted by some trusted third-party, perhaps. The third-party cannot forge any ledger entries, so what is the problem with this setup? What are Nakamoto's "main benefits" that are lost?

Firstly, there are two problems:

- The third party could delete a transaction, reversing history
- The third party could censor a transaction, i.e., refuse to enter it into the ledger.

And secondly, it's not just the third party itself who has this power, it's also the government who regulates them, or the hacker who infiltrates them. For Nakamoto (2008), using a trusted third party for this task loses some of the "main benefits" of the crypto setup because third parties have a real-world identity (a registered business, an IP address, etc.) and if known, these third parties could be censored by governments, hacked, or shutdown.

One of the key design goals behind bitcoin is censorship resistant digital cash. So, with this design goal in mind, how can a record of crypto-signed transactions that is both authoritative (in the sense that there is consensus on its veracity) and censorship resistant be created? Nakamoto provides a solution to this problem in the next part of the abstract:

> "We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power." [Nakamoto (2008), 1]

Bitcoin is a peer-to-peer network. It's flat. It is architecturally decentralised. There's no "bitcoin server" where the chain-linked blocks of transactions (transactions that are themselves also chain-linked via crypto signature) are centrally stored. Instead, the transaction record is stored redundantly by many nodes on the network. Anyone can be a node on the network anonymously – bitcoin is a "permissionless" network.

What does Nakamoto mean by "the network timestamps transactions"? Most people (especially people in financial markets) understand a timestamp to mean something generated by an accurate clock. But this, remember, is a peer-to-peer network, so it doesn't have a clock. The nodes on the network have clocks, but since these nodes could be anyone, the timestamp of any given node can't really be trusted. So how exactly does the network "timestamp transactions"?

What Nakamoto means here by "timestamp" is something less precise: the ordering of the blocks of transactions, i.e., this block of transactions came immediately after that block of transactions. This is ordinal time, a relative timescale. It is in this sense that the "network timestamps transactions." And how it does this is ingenious: "hashing them into an ongoing chain of hash-based proof-of-work."

This is where many people get lost. The basics are actually rather simple, but it is important to understand some preliminary concepts first. A "hash-based proof-of-work" is a solution to a problem, a hash problem. The "hash" refers to a branch of mathematical functions called "cryptographic hash functions," which have an interesting feature in that whatever data you put into one of these functions, they return a pseudo-random number of the same bit size. It's not really possible to predict what the function will return given a certain input, without actually computing the function yourself. Between inputs and outputs, there is no pattern.

For example, here is the SHA256 hash (the same hash function used by the bitcoin protocol) of the input "Goldman Sachs":

b0aad912e3a3d9c1be503c154c0580531709862a

Change that string by just one character and you get something entirely different: here is the hash of "Goldman Suchs":

a0b9a202da83ea581e0306f28115b7c6e10c8483

In bitcoin, the hash problem is: "input into the hash function (1) a number of transactions along with (2) the hash of the previous block of transactions, and (3) an arbitrary number N; if the hash function returns a value below some number D (called "difficulty", a varying number defined by the protocol), problem solved, if not, increment N and repeat." There's no way to solve this problem except through iteration (setting your computer to the task of running billions of hash computations until you solve the hash problem.

This is why it's called "proof-of-work." The problem was difficult to solve, it required the computer to do some work. But once it's solved, you can prove to someone else that you did the work to solve it. Just show them the data (a number of transactions plus

the hash of the last block) and that winning number N, and they can calculate the hash. If the hash value is the same below-D number that you say it is, you've proved that you solved the problem. The problem is hard to solve, but the solution is easy for others to verify.

This is how the bitcoin network timestamps transactions. The nodes on the network ("miners") collect transactions that bitcoin senders broadcast and each works at solving the hash problem over a set of transactions. Whenever a node solves the hash problem, it broadcasts the block of transactions along with the proof-of-work. The other nodes verify the work and start hashing on top of that block (i.e., including its hash in the input of the hash problem).

And this is what Nakamoto means by "forming a record that cannot be changed without redoing the proof-of-work." Nodes on the network build on top of the "longest chain" of blocks. If an attacker wanted to reverse the history, say, five blocks back, he or she would have to redo the proof-of-work of those five blocks before other nodes would start accepting that his version of history is the correct version (because it's the longest chain). And that's no mean feat. As Nakamoto states:

> "The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers." [Nakamoto (2008), 1]

This is a neat result. If every node follows the rule that the chain-linked set of blocks with the most work behind it is the blockchain, then every node's local copy of the blockchain will be exactly the same. And if an attacker wished to maliciously replace part of the "sequence of events witnessed" by the network (e.g., one where he made a big payment to someone) with an alternative version of history (e.g., one where he didn't make that payment), he would have to redo the latest work of the longest chain, and do this work at a faster rate than the rest of the network. Hence, he would need to control over 50% of the network's CPU power.[2]

And that, in a nutshell, is bitcoin's security guarantee. If you're comfortable believing that an attacker is unlikely to ever pull together more than half of the network's computing power, you can trust the veracity of the blockchain's record of transactions. Unlike with the case of a database hosted by a third party, there's no easy way for record entries to get "deleted" from the blockchain.

Here is a really important point to remember, however. All those hash problems that are being solved – the enormous amount of computational power that is "securing the network," as it is popularly described – are not securing the network in the way that, for instance, a computer that encrypts a message secures its contents from prying eyes. There is no fancy math behind the security of bitcoin. The only reason that a cryptographic hash function is used is that a hash-based proof-of-work problem has the property of being "hard-to-solve-but-easy-to-verify." You need that asymmetry in solution/proof; the network would grind to a halt if everyone had to redo everyone else's work. That's why bitcoin miners aren't spending all that computational power on something useful like, for instance, genome sequencing. With most useful computations, you generally have to trust that the computer did them correctly, the computer can't prove to you that it computed correctly. But with a hash problem you can easily prove that you did the computational work to solve it, even though the solution is utterly useless math.

So, the security behind proof-of-work isn't "based on math" (as some misleadingly say). Those hash computations are there for one simple reason: to make it expensive to offer a block of transactions to the network that the other nodes on the network will accept as valid. This is an economic model of security, not a cryptographic one. Proof-of-work requires an attacker to make a substantial capital outlay (in computing power and electricity) to have any chance of pulling it off.

THE DESIGN GOAL: CENSORSHIP RESISTANT DIGITAL CASH

Nakamoto envisioned a distributed, shared ledger of transactions based on a principle of "one-CPU-one-vote" (although today you need dedicated sha256 hardware, so it's really more like a computing oligarchy than a computing democracy, a discussion point that is outside the remit of this paper). One might ask: Why not have a similar set up but instead use the principle of "one-node-one-vote," thus sidestepping the expensive and wasteful proof-of-work?

The answer to that question is the single most important idea to take away from the bitcoin protocol. One-node-one-vote works only if you have a way of authenticating the real-world identity of the node, because otherwise a single attacker could just masquerade

2 In actual fact, researchers [Eyal and Sirer (2013)] have demonstrated that it is possible in theory to attack the bitcoin network with less than half of the network's computing power: the threshold is closer to 1/3 instead of 1/2.

as a number of different identities and gain control of the network, which can't tell whether 1000 nodes are really 1000 different people/entities or just one person behind them all, pulling the strings. This is called a Sybil attack[3] in the computer science literature, and authenticating node identity is one way of mitigating that attack vector. However, Nakamoto settled on a more ingenious solution, the hash-based proof-of-work that was explained above.

Remember Nakamoto's design goal: the creation of "censorship-resistant" digital cash. Prior to bitcoin's popularity, privately created electronic money existed in a hostile political environment, to put it mildly.[4] Authentication wasn't an option, because if the real identities of the nodes are known to all, governments could compel those nodes to censor transactions and apply KYC/AML procedures on the transaction senders, or, more extremely, just criminalise it and indict the operators behind the nodes. The "one-CPU-one-vote" idea behind hash-based proof-of-work is a solution that addresses the Sybil attack problem without relying on identity authentication. Instead of proving to the network that you're a unique flesh-and-blood person, you can prove to the network (without revealing your identity) that you've spent a lot of electricity and computing power, brute-forcing a solution to a meaningless math problem.

The bitcoin protocol is not only architecturally decentralised, it is also politically decentralised. The network has no gatekeepers, no permission is needed to join. The only admission criterion to contributing to the network's consensus is access to computational power.

"THE BITCOIN PROTOCOL IS NEITHER PERFECT NOR ANTI-FRAGILE"

At the beginning of this article, two main problems with using a ledger hosted by a trusted third party were pointed out:

- The third party could delete a transaction, reversing history
- The third party could censor a transaction, i.e., refuse to enter it into the ledger.

Nakamoto's hash-based proof-of-work beautifully solves the second problem. It is also designed to solve the first because bitcoin transactions are designed for irreversibility. And when bitcoin is cast in the role of distributed ledger platform for X (e.g., securities settlement), people are fond of describing the bitcoin blockchain as an "append-only distributed ledger for X."

But this is only a design goal, and because it is a design goal that has been subordinated to censorship resistance, the bitcoin protocol can provide no guarantees that this supposed "append-only" distributed ledger doesn't actually have a delete button accessible to an attacker who has a sufficient incentive and resources to attack the network and reverse blocks of transactions with impunity. Nakamoto (2008, 1) himself points this out in the abstract: "As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers." But if an attacker has access to more than 50% (actually, closer to 30%, see above) of the network's computing power, all bets are off.

In March of this year, Cornell University computer science professor, professor Emin Gün Sirer tweeted: "The #Bitcoin protocol is neither perfect nor anti-fragile. The main protecting force has been people's good will and lack of sophistication."

Emin is right. And this benign state of affairs is unlikely to persist if the bucket shops, which are today the only avenue for shorting bitcoins, are eventually replaced by professional derivatives markets. And it will certainly go away if billions of dollars worth of securities are represented through meta protocols on the bitcoin blockchain as some have eagerly extrapolated from the Nasdaq announcement. For then, attackers will have a way of constructing a scalable payoff for attacking the network: shorting the market in size. Acquiring a substantial portion of the network's hashing power is not an insurmountable goal. What is required is a sufficiently large monetary incentive to execute the attack. Putting billions of dollars worth of financial assets on the bitcoin blockchain materially changes an attacker's incentives.

Bitcoin transactions can be reversed if the attacker is willing to make the capital outlay to acquire the hardware and expertise and pay the electricity bill required to pull it off (bribing a few large mining pools is probably the path of least resistance). If the attacker is successful, the attack in theory costs nothing: the attacker collects the mining award of the blocks he solved, which "replace" the original transaction history, and which now is the chain with the most work behind it.

To the uninitiated, it might seem crazy that this ostensibly "append-only" distributed ledger that is the bitcoin blockchain contains

3 See https://en.wikipedia.org/wiki/Sybil_attack
4 See, for example, the Liberty Dollar case: https://en.wikipedia.org/wiki/Liberty_Dollar

an avenue for deleting history. After all, everyone saw those blocks of transactions before they were overtaken by the attacker's new blocks. Nobody will be fooled that the protocol's "network timestamp" corresponds to the ordering of transactions that actually occurred. But that's how the protocol works: "the" bitcoin blockchain is the chain of blocks with the most work behind it. This is the price you pay for the censorship-resistant design.[5]

THE BITCOIN PROTOCOL AND SECURITIES SETTLEMENT

The idea of "coloring" nominal quantities of bitcoin to represent security interests and piggyback a distributed ledger of financial assets on top of a politically decentralised digital cash system is wrong. Having "looked under the hood" of the bitcoin protocol, it is possible to see why.

To serve as a replacement for the legacy technology implementing registered, book-entry assets, a distributed ledger of financial assets will have to ensure a tight correspondence between what the ledger and the law say is the state of who-owns-what. This is obviously incompatible with a protocol based on anonymous transaction validators: the law will not treat a ledger record as authoritative if everyone knows that the current longest chain contains transaction blocks generated by an anonymous attacker. But the bitcoin protocol has no mechanism for dealing with this scenario, no mechanism for bringing ledger state and legal state back into alignment. How could it? Remember Satoshi's design goal: "censorship-resistant" digital cash. The price paid for that goal was a proof-of-work consensus model where the chain with the most work behind it is "truth" as far as the protocol is concerned.

The financial system and its regulators go to great lengths to ensure that something called "settlement finality" takes place. There is a point in time in which a trade brings about the transfer of ownership – definitively. At some point, settlement instructions are irrevocable and transactions are irreversible. This is a core design principle of the financial system because ambiguity about settlement finality is a systemic risk. Imagine if the line items of financial institution's balance sheet were only probabilistic. You own X of Y with 97.5% probability. That is, effectively, what a proof-of-work based distributed ledger gives you. Except that you don't know what the probabilities are because the attack vectors are based not on provable results from computers science but economic models. Should a settlement system be built on that edifice?

Of course not. And fortunately, it doesn't have to be because there are many ways to design distributed, shared ledgers. And it is unlikely that censorship-resistant securities transactions are the reason why financial institutions are looking at distributed consensus technology. Financial institutions' goals are rather different from Nakamoto's. Increased transparency is one, largely driven by the belief that regulators will grant concessions on capital charges for trades cleared through settlement systems that offer this. Efficiency through automating the back office is another. However, the main goal is probably increasing the speed of trade settlement.

From the experience of the author, this motivation perplexes many engineers, who understand well that distributed consensus technology is much slower than database technology. Proof-of-work protocols like bitcoin's are the slowest of the lot by far (and with only probabilistic ledger state to boot – censorship-resistance is expensive). But even far more efficient consensus algorithms will underperform the most basic relational database technology.

And yet it takes days to settle trades in book entry assets. This fact is only puzzling to those laboring under the mistaken assumption that custody accounting in the financial system is somehow centralised. It's not. Records are distributed throughout the system by thousands of different institutions, each one maintaining their own siloed accounts and constantly reconciling against each other to come to agreement on the global state of who-owns-what, or who-owes-what-to-whom. It is, in a sense, a form of distributed consensus: consensus-by-reconciliation. And consensus-by-reconciliation is very slow, expensive, and hard to automate. It is this technological infrastructure of consensus-by-reconciliation that the bankers, quite rightly, see being replaced by distributed, shared ledgers. This is a different problem from the one Nakamoto tried to solve, as a careful reading of Satoshi's abstract alone makes perfectly clear.

REGISTERED VERSUS BEARER ASSETS

Nothing in what has been discussed here is meant to take away from the inspired, brilliant solution that Nakamoto implemented for censorship-resistant digital cash. And, furthermore, that design goal is, in my opinion, a worthy one. Society should have digital cash that replicates the same anonymous and permissionless properties that are already enjoyed with physical currency.

5 When Nakamoto says that the longest chain "serves as proof of the sequence of events witnessed," I'm inclined to think he should have used the word "evidence" rather than "proof."

But a proof-of-work blockchain is only suitable as a distributed ledger for value that society is prepared to treat as a bearer asset. Physical cash is (almost) like this. A shop owner doesn't "due diligence" his customer to make sure that the $10 note the customer is about to hand over rightfully belongs to him. In practice, when it comes to physical cash, possession-is-ownership.

The same principle applies to the bitcoin blockchain. Possession (of a private key) is ownership (at least in the anarchic, code-is-law jurisprudence of the bitcoin protocol), regardless of how one came into possession, for there is no way for the blockchain to discriminate among spend transactions of coins obtained through legitimate trade, defrauding a counterpart (e.g., via a double-spend), or theft of someone's private key.

But the proposition that security interests and other property titles should also be cast in the same bearer asset mould will go nowhere. Few actually want this, and, in any case, few jurisdictions will actually allow it. In fact, it's looking increasingly likely that few jurisdictions will even grant bitcoins bearer asset status.

The advocates of putting property titles on the bitcoin blockchain will likely object at this point. They will say that through meta protocols and multi-key signatures, third-party authentication of transaction parties can be built in, and we can create a registered asset system on top of bitcoin. This is true. But what's the point of doing it that way? In one fell swoop, a setup like that completely nullifies the censorship resistance offered by the bitcoin protocol, which is the whole raison d'être of proof-of-work in the first place. These designs create a centralised transaction censoring system that imports the enormous costs of a decentralised one built for censorship-resistance – the worst of both worlds.

If you are prepared to use trusted third parties for authentication of the counterparts to a transaction, then there is no compelling reason for not also requiring identity authentication of the transaction validators as well. By doing that, you can forego the gross inefficiencies of proof-of-work and instead use a consensus algorithm of the one-node-one-vote variety, which is not only thousands of times more efficient, but also places a governance structure over the validators that is far more resistant to attackers than proof-of-work can ever be.

REFERENCES

- Brown, R., 2015, "Blockchain is where banks have the most obvious opportunity. But you ignore Bitcoin at your peril," Richard Gendal Brown: Thought on the future of finance, blog. Available at: http://gendal.me/2015/05/12/blockchain-is-where-banks-have-the-most-obvious-opportunity-but-you-ignore-bitcoin-at-your-peril/ and accessed August 15, 2015
- Eyal, I. and Sirer, E. G., 2013, Majority is not Enough: Bitcoin Mining is Vulnerable. Research Paper, Cornell University. Available at: http://arxiv.org/pdf/1311.0243v5.pdf
- Nakamoto, S., 2008, "Bitcoin: A Peer-to-Peer Electronic Cash System," white paper. Available at: https://bitcoin.org/bitcoin.pdf
- Nasdaq, 2015, "Nasdaq Launches Enterprise-Wide Blockchain Technology Initiative," press release, May 11. Available at: http://ir.nasdaqomx.com/releasedetail.cfm?ReleaseID=912196 and accessed August 15, 2015
- Skinner, S., 2015, "Repeat after me: Bitcoin Bad, Blockchain Good," Financial Services Club, blog. Available at: http://thefinanser.co.uk/fsclub/2015/05/repeat-after-me-bitcoin-bad-blockchain-good.html and accessed August 15, 2015

APPENDIX

A colloquial illustration of the Diffie-Hellman-Merkle key exchange and Blockchain

We begin by illustrating how a private and public key can be used to exchange information in a secret way, to avoid man-in-the-middle attacks. We then comment on the differences with Bitcoin Blockchain.

Public Key exchange (PKE)

A has to send a message to B that must not be deciphered by anyone except B, in case the message falls in wrong hands (someone in the middle). A and B need to share a secret code to transform the message.

This secret code needs to be known to both of them and no one else.

A uses B's public key, say KBpublic (accessible to anyone) and his own private key (secret, known only to A) KAprivate to create a mixed key KA1.

KA1 = calculation based on KAprivate and KBpublic.

Similarly, B uses A's public key KApublic (accessible to anyone) and his own private (secret, known only to B) KBprivate to compute

KB1 = calculation based on KBprivate and KApublic.

KA1 is sent from A to B and KB1 from B to A. Anyone intercepting KA1 or KB1 and knowing KBpublic and KAPublic wouldn't be able to get KAprivate or KBprivate by inverting the above calculations because this inversion is too hard computationally. In particular, B will not be able to compute KAprivate and A will not be able to compute KBprivate.

Now both A and B do a second calculation using their respective secret keys, getting

B computes: KA1B = calculation based on KA1 and KBprivate.

A computes KB1A = calculation based on KB1 and KAprivate

By the nature of the operations and by relevant commutative properties, KB1A and KA1B are the same key. So now both A and B share a key KB1A = KA1B that both can use to communicate secretly.

The information exchanged, namely KA1 and KB1, does not allow anyone intercepting it or the opposite party to find the secret codes of the sending party. The fact that only the mixed information KA1 and KB1 is exchanged and that separating the mixture is not possible in practice, due to computational difficulty, is at the basis of this public key encryption exchanges.

Publick keys and Blockchain

In Blockchains one does not actually use PKE for encrypting (nothing on a blockchain is encrypted). One instead uses them for digital signatures. Suppose I encrypt some message M with my private key. Now anyone can decrypt that message with my public key (so privacy isn't our goal here, obviously). And by decrypting that message, anyone can prove that I wrote M, which is why we call that a crypto signature.

So the idea of using PKE to implement digital cash is elegantly simple. Everyone's public key acts like a sort of account number. So if I want to pay X digital cash to you, I create a message/transaction that says "I, the owner of this public key K1, pay public key K2 X bitcoin" and then I sign that message with my private key. Now the transaction ledger can verify via crypto proof that I'm really the person who controls the K1 "account" and nobody can tamper with my instruction (because that would break the signature) so there's a mathematical proof that K1 instructs to pay K2 X coins.

The implementation details are more complicated (but elegantly so), but this is really the essence of it. This one aspect of blockchain tech is over 20 yrs old and is really quite simple.

It's the distributed consensus over a ledger of such crypto-signed transactions that's more deep and difficult and where the real innovation lies.

REVISITING CONCEPTIONS OF COMMODITY AND SCARCITY IN LIGHT OF BITCOIN

Konrad S. Graf

1. Introduction

Tradable bitcoin units viewed as discrete objects of human action are a new type of monetary phenomenon. They can even appear to elude trusted monetary typologies. This paper seeks to clarify their economic nature by reexamining core theoretical concepts with bitcoin held in mind next to more traditional examples.[1] It also distinguishes economic-theory and property-theory senses of scarcity, and seeks to better differentiate scarcity from tangibility or materiality. These steps help overcome interpretive challenges in considering bitcoin in relation to the monetary classification scheme pioneered in Ludwig von Mises's *The Theory of Money and Credit* (TMC).[2] They may also help inform emerging debates in progress as to whether and in what sense bitcoin units should or should not be considered legitimate objects of legal ownership under a rigorous approach to the foundations of property theory.

With these proposed pieces in place, the paper next examines bitcoin using a typical set of criteria for explaining the historical-evolutionary strengths of metallic coins as media of exchange. How does bitcoin fare on a representative list of criteria used to describe what gives certain types of market goods competitive advantages in a monetary role? It concludes by recalling the importance of applying realistic comparative methods and avoiding comparisons of real options against idealized imaginary versions of other options.

The focus is on the perspective of individual actors and discrete marginal objects of action (both tangible and intangible "objects"). I address technical-system, payment-network, and social-system perspectives in *On the origins of Bitcoin: Stages of monetary evolution* (October 2013) and my three-part *Bitcoin Decrypted* video lecture series (December 2013). These treatments build on the action-theory foundations developed here in keeping with the Misesean tradition of methodological individualism, in which systemic treatments of social phenomena are to remain rooted in action analysis.

---

[1] I attempt to follow general usage advice in using upper-case 'B' for protocol, network, or overall phenomenon, and lower-case 'b' for currency. Lower-case bitcoin is sometimes used in an uncountable sense, as in water or oil. The countable plural usage of "bitcoins" is a confusing and unresolved and evolving linguistic issue due to the increasingly large exchange value of a "whole bitcoin" (=100 million satoshis). For now, I sometimes resort to "bitcoin units" when it is important to unmistakably include any tradeable amount, regardless of exchange value.

[2] Ludwig von Mises. 1953 [original German, 1912]. *The Theory of Money and Credit*. New Haven: Yale University Press.

2. Epistemological dualism and the role of terminology

In taking a strictly subjectivist position on the nature of goods, the fact that bitcoin units might be described as "merely" the current status of accounting entries in the ubiquitously duplicated block chain record, and therefore not "really" goods at all, raises less difficulty than it might at first appear. Of interest for action-based economic theory is the interpretive observation that large numbers of market actors on a global scale are actually treating these units as a scarce economic good in general and as a medium of exchange in particular, as demonstrated through their actions and choices. Bitcoin units might be viewed as property titles, but if so, they are self-referential "titles" to nothing other than themselves as tradable goods.

By way of illustration, one might quip about the historical trading of a commodity money such as silver that, just behind the outward surface, the metal is "really" just one particular pattern by which sub-atomic particles are arranged in nature, resulting in certain observed physical properties. Such context-shifting commentary, however, would not seem to advance our understanding of the monetary phenomena observed. The Misesian method in economics takes no *direct* interest in such matters in the sense that it calls for a strict differentiation between those methods and fields concerned with the study of human action and those concerned with the study of things and (non-action) behaviors. Economics is part of the study of action itself and its extended implications for social analysis.[3] The objective natures of the objects of such action are of interest to the sciences of human action only by secondary extension for use in the specific interpretation of definite actions and patterns observed in specified times and places.

---

[3] In more technical terms, this is the dualist distinction between 1) the teleological concepts of action such as ends, means, and meanings and 2) the objective, causal relationships of the natural sciences concerning the realms of the dimensionally measurable including matter, space, and energy.

In 2011, I began using "action-based" as a synonym for "praxeological" in the sense defined by Mises, starting in "Action-Based Jurisprudence: Praxeological Legal Theory in Relation to Economic Theory, Ethics, and Legal Practice," *Libertarian Papers* 3, 19. In short form, see also, "Misesian action theory is an approach to social theory, not just economics," 20 February 2013, with "(Misesian) action theory" substituting for "praxeology."

On the foundations and methods of action theory, see in particular: Mises. 2006 [1962]. *The Ultimate Foundation of Economic Science: An Essay on Method.* Indianapolis, IN: Liberty Fund; and Jörg Guido Hülsmann. 2003. "Facts and Counterfactuals in Economic Law." *Journal of Libertarian Studies* 17 (1): 57–102.

If no existing category in a given monetary typology proved sufficient to contain bitcoin, a new category might have to be appended. In investigating a new case, terms and categories should facilitate understanding rather than hinder it. In developing his terminology in Chapter 3, "The Various Kinds of Money" in TMC (50–67), Mises sought to employ terms that would facilitate economic analysis more effectively than the conventional and positive-law terms of the time (59–60).

> Our terminology should prove more useful than that which is generally employed. It should express more clearly the peculiarities of the processes by which the different types of money are valued. [It should also help to overcome] the naive and confused popular conception of value that sees in the precious metals something "intrinsically" valuable and in paper credit money something necessarily anomalous. Scientifically, this terminology is perfectly useless and a source of endless misunderstanding and misrepresentation. (61–62)

I do not believe that Mises's typology from TMC necessarily requires any fundamental revision to account for bitcoin, though even if it did, this should not be considered problematic. The purpose of a typology is to helpfully set forth the monetary phenomena observed in a given time and place in a way that is relevant to the particular investigations being undertaken.

It may be possible to account for bitcoin within the TMC typology by taking a further step in the direction of a strictly dualistic action theory. This is the same direction of refinement that gave rise to those classifications to begin with as Mises pursued his career-long process of moving economic theory away from objectivized constructs and toward an ever more careful grounding in action analysis.[4] Mises warned sternly in 1912 that:

> The greatest mistake that can be made in economic investigation is to fix attention on mere appearances, and so to fail to perceive the fundamental difference between things whose externals alone are similar, or to discriminate between fundamentally similar things whose externals alone are different. (62)

In what follows below, I retain the TMC categories and seek to refine the popular understanding of what "commodity" means toward a more strictly economic-theory sense rather than a more intuitively accessible materialistic or historical one. I have outlined an alternative monetary typology that is based on legal-status differentiations elsewhere, near the end of *Bitcoin Decrypted*. I consider that approach and the one below compatible, highlighting different aspects of the same phenomena.

[4] Hülsmann. 2003b. "From Value Theory to Praxeology," Introduction to the third edition of *Epistemological Problems of Economics* by Ludwig von Mises. Auburn, Alabama: Mises Institute.

3. Commodity money viewed as an economic-theory concept

Among its many other contributions, Peter Šurda's 2012 thesis, *Economics of Bitcoin: Is Bitcoin an alternative to fiat currencies and gold?*[5] examined bitcoin in terms of Mises's typology from TMC. Having already given some initial thought to the matter, upon first reading Šurda's account, I discovered that up to a certain point, he and I had interpreted bitcoin in largely the same way.

He rejected one candidate after another as a place for bitcoin within the TMC scheme (23–28). It is not any kind of money substitute, as it is not "redeemable" for any more fundamental unit. Even *within* Mises's "money in the narrower sense," that is, senses other than money substitutes, bitcoin is not credit money, as no creditor/debtor relationship exists. Finally, it is not fiat money, as it lacks any legal-tender status or other state-sponsored privileges, stamps, or certifications. Šurda and I had each arrived independently at just one possible candidate: commodity money.

Yet for many observers, as visible in online debates, this initially seemed like it could not be quite correct either. Some found it more intuitive to *start* by rejecting commodity money as a possibility, and then trying to make analogies to other categories, including fiat money and token money.

This is understandable. If one has in mind a conception of commodity that includes materiality as an essential characteristic, it would be impossible to imagine purely informational bitcoin as being one. True, in certain other contexts, "commodities" can have a quite broad meaning. In the broadest usage in purchasing-power theory, commodities are the euphemistic label for everything that is *not* money—all that against which money prices are paid. Nevertheless, in a "commodity money" context, a commodity is usually thought of in its narrower and more common meaning: a fungible, divisible material or product, such as metal, oil, grain, or these days, even interchangeable "commodity" memory chips or other general-purpose electronic components as contrasted with customized components.[6]

In the face of this apparent impasse, Šurda next proposed several considerations. First, since he had argued that bitcoin is not a money (yet), but a secondary medium of exchange (22), it need not necessarily fit on a chart of money. Yet he also recognized that this was not a long-term solution. What if bitcoin *did* grow to qualify as "money" in the future?

---

[5] Peter Šurda. 2012. Vienna University of Economics and Business.

[6] In *On the origins of Bitcoin* (October 2013, 2–3), I argue that Carl Menger used the concept of commodity in an analysis of *pricing conditions* for various classes of goods (specialty versus general purpose), and that the materiality of the goods considered was more as an historical association than a characteristic essential to his topic. See Menger. *On the origins of money*. 2009 [1892]. Auburn, Alabama: Ludwig von Mises Institute. Translation by C. A. Foley.

In a later post, he stated perhaps the most important point of all:

> The issue...is not some abstract classification for its own sake. The purpose of the classification system provided by Mises is to assist in the economic analysis of trade, money supply, price building, liquidity and so on. From this perspective, if we insist that we must keep the number of categories the same that Mises used, the economically closest category of Bitcoin would be commodity money. [7]

After considering bitcoin in light of traditional definitions of money and medium of exchange, particularly the imprecise definition of money as a "commonly used" medium of exchange, I have come to identify money as the unit of pricing, accounting, and economic calculation in a given societal context. I define medium of exchange as a good used for payment of money-denominated prices in indirect exchange transactions. Bitcoin currently qualifies under the second category and not under the first. However, I see no reason that it could not begin eventually to qualify under the first in certain times and places if and as adoption continues to expand.[8]

In search of still further clarification about bitcoin and the concept of commodity money, we turn to the use of language and its context. In language, meaning comes first; words follow along as best they can. Concepts are one thing; the words used to signify them another.[9]

TMC is a translation of Mises's 1912 *Theorie des Geldes und der Umlaufsmittel*.[10] "Commodity money" was the term used to translate the German *Sachgeld.* Although some issues have been found with the TMC translation, including a rather serious problem with the title,[11] "commodity money" seems a perfectly reasonable translation in this case. I am aware of no reason to think that Mises

---

[7] Šurda. 12 March 2013. "The classification and the future of Bitcoin." *economicsofbitcion.com.*

[8] Graf. 14 September 2013. "Bitcoin as medium of exchange now and unit of account later: The inverse of Koning's medieval coins." *konradsgraf.com.*

Another definition of money would be "the most liquid good in a given societal context." In most, and perhaps all cases, such a good is also used as the unit of account. Units of this good, more than any other, can be observed to trade in varying numerical relationships directly against all other market goods and services, giving rise naturally to a pricing role. The most liquid good is in this way also most likely to be used as a unit of pricing and accounting. Next to the abstract "most liquid," the latter descriptors have the practical advantage of being readily identifiable in each empirical situation based on their prominent role in price labeling.

[9] A good translator works at the level of the concepts and meanings that the various words are employed to convey—at times somewhat imperfectly—in specific communicative contexts.

[10] Munchen und Leipzig: Ferlag von Duncker & Humblot.

[11] Hülsmann. 2012. "The Early Evolution of Mises's Monetary Thought," *Theory of Money and Fiduciary Media: Essays in Celebration of the Centennial.* Auburn, Alabama: Mises Institute.

would have objected, or did object, to this choice. In *Nationalökonomie*,[12] the 1940 German precursor to *Human Action*, many instances of *Sachgeld* are accompanied by the usual examples of gold and silver, which also serve as the stock examples of commodity money in *Human Action*.

In brainstorming about the classification of bitcoin, however, the two-part compound construction of *Sachgeld* suggested to me connotations that "commodity money" did not. *Die Sache* is a "thing," in either a concrete or abstract sense, which contrasts with *das Ding*, "thing" only in an objective physical sense. Alternative senses of *die Sache* and associated compounds readily include such abstract senses as "the matter at hand," "the facts of the situation," and "the main or most important point or issue." *Sachgeld* in modern dictionaries comes across as any object (or even animal or slave)[13] that was historically used as a medium of exchange, or simply the earliest forms that money took[14] (which happen also to have preceded the sequential evolution of money substitutes).

Sachgeld, in this most literal construction, looks like "thing-money." But recall that *die Sache* taken alone carries the abstract sense of thing or fact. A "thing" is usually considered tangible, but unlike commodity in its usually assumed meaning of a fungible physical material, "thing" can also easily cover abstract senses such as "matters at hand," "conditions," etc., as in, "the thing is…" or "How are things going?" or "It is a curious thing."

This suggested to me a way to proceed with the classification of bitcoin: by clarifying the conception of *Sachgeld* in a more strictly economic (action-based) rather than objectivistic (falsely placed material) sense. "Commodity money," in this view, is the monetary "good itself," without any intermediation such as a fixed-rate substitution promise or other credit relationship.

Such a clarification of the term commodity money would also be in keeping with the overall direction of progress in economic theory in distinguishing ever more carefully between action-based teleological concepts and the objective characteristics of the particular means that actors employ. If we take the central *economic* (as opposed to historical-descriptive) meaning of *Sachgeld* to be "money in itself," this would still contrast with all of the other categories in the TMC scheme in the same way that a materialistic understanding of commodity would, except that the more abstract sense can also account for bitcoin. Money in itself contrasts with money by extension—extension through such intermediaries as fixed-rate substitution promises, credit relationships, and any variation of the trust, reputation, or "full faith and credit" of some specified institution.

---

12 Mises. 1940. *Nationalökonomie: Theorie des Handelns und Wirtschaftens.* Genf: Editions Union.

13 wirtschaftslexikon24.com/d/sachgeld/sachgeld.htm

14 zahlenbilder.de.

Much as a circulating silver coin once functioned directly as "money in itself," and was not "backed" by anything, a bitcoin unit is likewise not backed by anything. It is not a perfect or imperfect substitute for anything else. From the point of view of economic actors using it, bitcoin *is the tradable good itself*. From a strictly action-theory point of view, no intermediating substitutes stand between the good itself and its end user/controller. Fiat money is also in one sense treated as a good in itself, but it relies heavily on being "backed" by the force of law and monopolistic status. This is part of what led me to develop the legal-status based categorization introduced in *Bitcoin Decrypted*. "*Sachgeld"* can—and bitcoin famously does—trade on the open market in a monetary role with no special contractual, legal, or legislative status whatsoever.

Moreover, the characteristics of bitcoin itself do not suggest a similar scope of demand for such money substitutes as have historically grown up around metallic currencies. Notably, the widespread historical use of such paper-note and account-entry substitutes was an essential element in setting up the long-term conditions for the emergence of fiat money as the links between commodity monies and their substitutes gradually degraded with progressive institutionalized corruption.

With bitcoin, such substitutes are possible; they just do not appear to necessarily add value. By adding superfluous derivative- and counterparty-risk layers, they can even subtract it. The bankruptcy of a centralized bitcoin exchange, such as the Mt. Gox collapse of February 2014, is a prime example of the kind of counterparty risk that the Bitcoin protocol itself was designed to eliminate.[15] One way that this counterparty risk functions in this case is that customers of a centralized exchange business do not maintain direct control of their bitcoin, but instead trade it for credits on an internal corporate accounting system. They then rely on the particular quality of this third-party managed internal system to the extent that they leave balances in it.

When this exchange collapsed, it became clearer to more observers that customers had been holding, not bitcoin, but bitcoin substitutes, Goxcoins, that is, Mt. Gox-brand bitcoin account credits. It is important to note that the Mt. Gox collapse is a company-specific failure and has no systemic implications of the kind associated with highly regulated and cartelized conventional financial systems.

4. Intellectual context for the TMC typology

For an initial check on how well this specification of the definition of commodity money toward a more strictly economic-theory sense might mesh with the context in which TMC appeared and its major contributions, we turn to Professor

[15] See the more detailed discussion of these points in Graf. 27 February 2014. "MtGox fiasco highlights advantages of Bitcoin and damage from regulation." *konradsgraf.com*.

Hülsmann's definitive intellectual biography, *Mises: The Last Knight of Liberalism*.[16]

> In dealing with the nature of money, Mises relied heavily on the work of Carl Menger. The founder of the Austrian School had shown that money is **not to be defined by the physical characteristics** of whatever good is used as money; rather, money is characterized by the fact that the good under consideration is (1) a commodity that is (2) **used in indirect exchanges**, and (3) **bought and sold primarily for the purpose of such indirect exchanges**. (215)

Many readers might ordinarily assume the words "good" and "commodity" point to physical characteristics. However, note that this paragraph emphasizes the functional *economic* characteristics of money for actors. Look for the action verbs: *used, bought* and *sold*. Moreover, "physical characteristics" are specifically singled out as factors on which money is "not to be defined."

In quickly reviewing Mises's typology of monetary objects, Hülsmann notes that:

> [Mises] distinguished several types of "money in the narrower sense" from several types of "money surrogates" or substitutes. **Money in the narrower sense is a good in its own right**. In contrast, money substitutes were legal titles to money in the narrower sense. They were typically **issued by banks** and were **redeemable in real money** at the counters of the issuing bank. (216–17)

"A good in its own right" is reminiscent of our proposed "money itself" concept. Although bitcoin substitutes, such as exchange account credits, exist, bitcoin itself is traded and held directly. It trades at freely floating rates against all other goods, services, and monies. Use of bitcoin substitutes is wholly optional on a user-by-user basis and entails a mix of pros and cons at the margin. Bitcoin itself is not the substitute in such cases, but the good itself, that which account credits substitute *for*.

Mises, in developing his monetary theory in TMC, was also arguing against the assignment theory of money, which holds that money has no real value of its own, but merely functions as a receipt that facilitates deposits and withdrawals on the "social warehouse" of goods. Money, in this view, is a veil, functioning as a claim ticket exchangeable for other goods, but not a good itself.

Hülsmann explains:

> Mises's great achievement in his *Theory of Money and Credit* was in **liberating us from the veil-of-money myth**...Mises could even rely on Menger's theory of cash holdings, which already contained, in nuce, the insight that money **is itself an economic good and not just representative of other goods**. (2007, 237)

Eugen von Böhm-Bawerk had framed it this way in an early-1880s lecture:

[16] Hülsmann. 2007. *Mises: The Last Knight of Liberalism.* Auburn, Alabama: Mises Institute.

> Money is by its nature a good like any other good; it is merely in greater demand and can circulate more widely than all other commodities. Money is no symbol or pledge; it is not the sign of a good, but bears its value in itself. It is itself really a good.[17]

Hülsmann explains the role of Mises's strict terminology in TMC in countering the prevailing assignment theory of money:

> To combine these elements into one coherent theory required a radical break with time-honored pillars of monetary economics, in particular, with the classical tradition of presenting money as a mere veil. Mises was fully conscious that this was the key to his theory, which is why, in an introductory chapter of his book [TMC, Chapter 3], he engaged in the somewhat tedious exercise of distinguishing various types of money proper (money in the narrower sense) from money substitutes. **It was these substitutes in fact that were the sort of tokens or place holders that Wieser and the other champions of the assignment theory tacitly had in mind when they spoke of money**...While it is true that the value of a money substitute corresponds exactly to the value of the underlying real good (for example, one ounce of gold), **the value of the gold money itself does not correspond to anything**; rather it is determined by the same general law of diminishing marginal value that determines the values of all goods. (237)

The rise of bitcoin a century after TMC has provided a fresh opportunity for revivals of the veil-of-money approach, and along with them, fresh opportunities to follow Mises in refuting it.

In sum, Mises had argued that money was not just a placeholder for other goods; it was one good trading for other goods on the market. Moreover, he differentiated *Sachgeld* within "money in the narrower sense," contrasting it with circulating debt instruments (credit money) and monies that depend on some official certification or special legislative status (fiat money). *Sachgeld*, while discussed in terms of its material, historical instantiations, thus served more abstractly as a sub-category of "money in the narrower sense" that did not rely on any contractual (credit) or other institutional (fiat) legal status.

One of the reasons a monetary good gains value is that its relatively higher liquidity[18] gives rise to an increased value as a hedge against uncertainty. If no uncertainty existed, there would be no need to hold cash balances. In the real and uncertain world, however, one does not know in advance exactly *what* one will want to buy, when, or from whom, but one typically does expect strongly *that* one will want to buy something sometime from someone. The holding of

---

[17] As cited in Hülsmann 2007, 235.

[18] As Šurda often points out, this was Menger's "saleability at economic prices." In, *On the origins of Bitcoin*, I emphasized Menger's distinction between the degree of difference between the relative positions of buyers and sellers. With highly "saleable" goods such as commodities, their positions are very similar; with specialty goods, more divergent.

cash balances can be understood as a forward-looking measure one takes in relation to this degree of perceived uncertainty.[19]

The more liquid the good, the better market participants expect it to enable them to purchase not-yet-specified goods and services at not-yet-specified future times. As more and more market participants around the world accept bitcoin—and new ones begin to do so daily—its utility in this uncertainty-hedge role grows. This is particularly so if it is paired with a user expectation that the exchange value of each unit is likely to rise over the medium- to long-term due to the combination of expanding global demand and the Bitcoin protocol's strict, asymptotic unit-growth trajectory.

Many critics of bitcoin cite its high current short-term exchange rate volatility, as if this early-stage state of affairs should permanently doom the project. Such critics do not typically also explain why holders of monetary-unit balances should not also take into account other salient medium-term empirical data next to short-term volatility. For example, the exchange value of bitcoin against US dollars at the end of 2013 was 56 times higher than it was at the beginning of 2013—the greatest annual appreciation recorded for any asset ever.[20]

Holders of various monetary-unit balances should reasonably be expected to contrast such developments with the relatively steady *decline* in the purchasing power of all fiat monies at varying rates, however steady or unsteady. Depending on a given decision-maker's expected timeframes for future purchases, short-, medium-, and long-term value expectations will be weighed in various configurations in deciding what balances of which tradable monetary units to hold over which durations. It is a relatively simple matter to understand that some market actors might perceive a potential medium- to long-term advantage in holding certain balances of a unit that the user expects to *rise* in value at a less consistent pace next to balances of other units that the user expects to *decline* in value at a more consistent pace.

Whatever the future brings, for today, bitcoin is traded directly as itself in a monetary role. It is digital *and* it is impossible for any given party, such as a central bank board or corporate issuer, to manipulate its total supply. This is critical, because one of the most important monetary issues of the foregoing centuries has been the expanding ability of money producers to manipulate the money supply to the advantage of their favored constituencies at the expense of other, less favored ones.[21]

---

[19] Hans-Hermann Hoppe. 14 May 2009. "'The yield from money held' reconsidered." *Mises Daily.*

[20] Coindesk. 26 February 2014. "State of Bitcoin 2014." (4).

[21] Hülsmann. 2008. *The Ethics of Money Production.* Auburn, Alabama: Mises Institute. mises.org/document/3747/The-Ethics-of-Money-Production.

As Mises wrote, “It is not just an accident that in our age inflation has become the accepted method of monetary management. Inflation is the fiscal complement of statism and arbitrary government (TMC, 428).” He also explained the related social-protective advantages of having precious-metal coins circulate physically:

> Gold must be in the cash holdings of everybody. Everybody must see gold coins changing hands, must be used to having gold coins in his pockets, to receiving gold coins when he cashes his pay check, and to spending gold coins when he buys in a store. (450)

This might seem to be the definitive Misesian endorsement of circulating metallic coins. Yet as Hülsmann notes, “Mises had not become a gold bug. He had no fetish about the yellow metal or any other metal” (2007, 922). Hülsmann then points to the *reasons* behind Mises’s proposal—to help counteract inflationary policies. Mises had explained that:

> What is needed is to alarm the masses in time. The working man in cashing his pay check should learn that some foul trick has been played upon him. The President, Congress, and the Supreme Court have clearly proved their inability or unwillingness to protect the common man, the voter, from being victimized by inflationary machinations.
>
> The function of securing a sound currency must pass into new hands…Perpetual vigilance on the part of the citizens can achieve what a thousand laws and dozens of alphabetical bureaus with hordes of employees never have and never will achieve: the preservation of a sound currency. (TMC, 451–52)

In Bitcoin, the function of securing users against unit inflation rests with cryptography and protocol definitions. Engaging in perpetual vigilance is the primary role of both the distributed global mining network and open-source development communities. The function of Mises’s having of “gold coins in everybody’s pockets” is fulfilled in that users maintain direct control of signing keys, such that there is no question as to how much bitcoin each person and entity controls out of a strictly regulated and publically verifiable total quantity in existence at any given time.

5. Meanings of scarcity; its differentiation from materiality

Precious metals bound together the qualities of scarcity and tangibility in a monetary context over many centuries. In further considering bitcoin and monetary theory, the concepts of goods, scarcity, and tangibility must be carefully differentiated.

What if factors other than tangibility, such as relative stability of total supply, durability, and divisibility, were always the *essential* factors regarding commodity money? What if tangibility was a sort of monetary “inactive ingredient,” a “material carrier” for *other* qualities that had always been the essential monetary characteristics? If so, perhaps these qualities could also be

delivered in previously unexpected ways other than through grounding in tangible materials.

Digital goods have brought the separability of goods from materiality front and center in the modern world. To apply these concepts to bitcoin, we revisit their various senses and definitions. Not only can bitcoin be viewed in light of theory, but theory revisited in light of bitcoin.

Most digital goods, such as song or text files, can in principle be copied *ad infinitum*. This was the essence of the digital-information revolution. Unlimited numbers of people could use copies at the same time without direct mutual interference or degradation of other copies. Unlike with the transfer of a physical object, such as by theft, a *copy* could be made without the original disappearing. Moreover, any copy could itself become a new "original" from which more copies could be made in a cascading process. Much the same applies to the emulation of practices seen or ideas heard in person, but it was the advent of mass digital replication that made this distinction increasingly significant.

Mass digital replication dealt a crushing blow in certain areas to an age-old adversary—inherent or natural scarcity. In response, however, a legal and technical scramble to create and expand *artificial* scarcity ensued. The chief methods have been expanding legislation and enforcement, ever more draconian and elaborate software license terms, and the application of digital rights management (DRM) technologies. These developments brought the dusty old issue of "intellectual property" out of the obscure corners of law libraries.

To make sense of this odd scene in a principled way called for a fresh look at basic social-theory concepts. As one step in this effort, Jeffrey Tucker and Stephan Kinsella in "Goods, scarce and nonscarce,"[22] focused on distinguishing perfectly copiable goods, such as ideas, methods, and most digital goods, labeling them "nonscarce goods." They quoted from Kinsella's "Against Intellectual Property" (2001), which addresses the relationship between tangibility, scarcity, and the core social function of property rights. Kinsella had asked:

> What is it about tangible goods that makes them subjects for property rights? Why are tangible goods property?...it is these goods' scarcity—the fact that there can be conflict over these goods by multiple human actors. The very possibility of conflict over a resource renders it scarce...the fundamental social and ethical function of property rights is to prevent interpersonal conflict over scarce resources. (19)

This sense of the word scarcity is a social-relational one. The term "rival good" also describes this. A rival good is one that different parties *could not use* simultaneously for different incompatible purposes without coming into conflict with one another over these purposes. For example, one person *cannot* drive from Rome to Vienna while another drives from Sydney to Brisbane *in the same*

[22] 25 August 2010. *Mises Daily.*

car. Notice that this is not a normative concept, but a descriptive one pertaining to the relationship between the nature of certain types of goods and their objective employability. This sense of the word scarcity is grounded in the property-theory reasoning of Hans-Hermann Hoppe, who wrote:

> insofar as goods are superabundant ('free' goods), no conflict over the use of goods is possible and no action-coordination is needed...To develop the concept of property, it is necessary for goods to be scarce, so that conflicts over the use of these goods can possibly arise. [23]

Yet the word scarcity carries other meanings. It is used in economic theory as a necessary attribute of *any* economic good, part of the definition of what a good *is*. It was in this broadest sense that Mises emphasized how the concept of a means only arises in relation to the concept of action:

> Means are not in the given universe; in this universe there exist only things...Parts of the external world become means only through the operation of the human mind and its offshoot, human action...**It is human meaning and action which transform them into means.**
>
> Means are necessarily always limited, i.e., scarce with regard to the services for which man wants to use them. **If this were not the case, there would not be any action with regard to them.** Where man is not restrained by the insufficient quantity of things available, there is no need for any action. (1998, 92–93)

Compounding the potential for confusion, in everyday usage, "scarce" has yet a third meaning of "in short supply" or "not enough to go around" relative to an assumed normal or ideal baseline supply. This evaluative sense differs from the two distinct descriptive senses above.

Tucker and Kinsella mentioned that tangibility is not necessary for scarcity, citing airspace and radio waves as examples—one transmitter can interfere with the signal from another. While the practical conclusion seemed to be that tangibility and scarcity do coincide in almost all cases, the authors left no doubt about the key point: "The term scarcity here...means that a condition of contestable control exists for anything that cannot be simultaneously owned: **my ownership and control excludes your control**."

In strictly economic-theory terms, one must still act to obtain even a "nonscarce" copy of an *economic good*, by definition. For example, one must still click on one free file icon rather than another, displaying choice and preference through this action, and making the clicked-on file a means and the runner-up file an opportunity cost. In the property-theory sense, however, even a non-good can be scarce, which is impossible in the economic-theory sense. Yet once again, Tucker and Kinsella had made their intended sense for scarcity clear:

---

[23] Hoppe. 2010 [1989]. *A Theory of Socialism and Capitalism.* Auburn, Alabama: Mises Institute. 235.

> Something can have zero price and still be scarce: a mud pie, soup with a fly in it, a computer that won't boot. So long as no one wants these things, they are not economic goods. And yet, in their physical nature, they are scarce because **if someone did want them, and they thus became goods, there could be contests over their possession and use**. They would have to be allocated by either violence or market exchange based on property rights.

Applying the dualist dividing line clarifies why airspace and radio waves qualify as scarce in this sense even though they are not material. The dividing line is whether the concept being addressed belongs to the realm of human meaning—including valuations, ends, and means—or to the realm of that which is physically measurable in dimensional space.

The subtle difference in the meaning of scarcity in these uses within economic theory and property theory reflects the respective clarification tasks at hand. Economic theory is concerned with action as such, which only individual actors can take (Crusoe). Property theory is concerned with individual action *in its capacity as occurring* in a social context of other actors (Crusoe plus Friday on up). The economic-theory sense of scarcity is used in considering Crusoe alone, while the property-theory sense can begin to also be used in considering the possible classes of interactions between Crusoe and Friday. And here is where the use of the term "rival" could help head off confusion, as rivalry is an inherently social-interactive concept.

Property rights are a purely social phenomenon. With Crusoe and Friday situations onward, social action theory posits binary action possibilities of either cooperation or violent conflict. These are differentiated by consent, and can most simply and intuitively be described as theft versus non-theft relationships. These encompass a descriptive categorical binary of all possible human interactions. Some investigators have selected this binary as being especially valuable for social analysis.[24]

Confusion in discussions of scarcity could also arise from the use of the term "free goods." In the economic-theory sense, free goods are not really goods at all, but the background conditions of action. They are not means in themselves within an intentional structure of action. Murray Rothbard put in this way:

> The *means* to satisfy man's wants are called *goods*. These goods are all the objects of economizing action...The common distinction between "economic goods" and "free goods" (such as air) is erroneous...air is not a means, but a general condition of human welfare, and is not the object of action. (2004, 8)

[24] For examples, see: Frédéric Bastiat. 2007 [1850]. *The Law*. Auburn, AL: Mises Institute; Hoppe 2010 [1989]; Hülsmann. 2004. "The A Priori Foundations of Property Economics." *The Quarterly Journal of Austrian Economics* 7 (4): 41–68; and Murray N. Rothbard, [1962, 1970] 2004. *Man, Economy, and State, with Power and Market.* The Scholar's Edition. Auburn, Alabama: Mises Institute. 79–94.

Air would not usually count as a means for a jogger unless that jogger was an obsessive economist who had in mind "using" air to go jogging. The air outside under normal circumstances is a background condition, but not itself an object of action, and therefore not a good, unless its supply or quality is threatened.

6. Goods and "renditions of services;" rival scarcity defined

To further clarify underlying concepts before applying them to bitcoin, we consider the concept of "good" itself more directly. A good is something that serves as a means within the structure of human action. This was already explained in Eugen Böhm-Bawerk's 1881 paper, "Whether Legal Rights and Relationships Are Economic Goods."[25] Gael J. Campan elaborates the subjectivist conception of a good that Böhm-Bawerk advanced:

> While scarcity is commonly referred to as an essential feature of an economic good, this must not be understood purely in a physical sense, i.e., a fewer number of items compared to the quantity of others. Indeed, if all means are scarce by definition, it is specifically because they are limited **with respect to the actual ends that they are capable of satisfying**...The characteristics of a good are **not inherent in things** and not a property of things, but merely **a relationship between certain things and men.**
>
> The thing named a *good* must have useful properties, which is not to be understood in a strictly physical sense.[26]

As quoted by Campan, Böhm-Bawerk wrote:

> Whatever importance we accord to the corporeal objects of the world of economic goods derives from the importance we attach to the satisfaction of our wants and the attainment of our purposes...It is the renditions of service rather than the goods themselves which, as a matter of principle, constitute the primary basic units of our economic transactions. And **it is only from the renditions of service that the goods, secondarily, derive their own significance**. (24)

We have seen that scarcity in the rival, property-theory sense pertains not to whether something is a good or not in the broader economic-theory sense, but rather to the native potential for rivalry and the presence or absence of the attributes of copiability and simultaneous shareability. Since the broader economic concept of scarcity is already contained within the definition of a good, the narrower property-theory sense appears more useful for the current tasks.

---

[25] Böhm-Bawerk, Eugen von. 1962 [1881]. "Whether Legal Rights and Relationships are Economic Goods." *Shorter Classics of Eugen von Böhm-Bawerk*. South Holland, Illinois: Libertarian Press; originally, "Rechte und Verhältnisse vom Standpunkte der volkwirtschaftlichen Güterlehre." Innsbruck, Austria: Verlag der Wagner'schen Universitäts-Buchhandlung.

[26] Gael J. Campan. 1999. "Does Justice Qualify as an Economic Good?" *The Quarterly Journal of Austrian Economics.* 2, 1 (Spring): 21–33.

Building on this property-theory sense of scarcity, a nonscarce good, or nonrival good, is **a good that is copiable with perfect remainder of the original and useable by multiple actors simultaneously without mutual interference**.

If the two travellers from our earlier example each had a separate car, each could drive from Rome to Vienna and from Sydney to Brisbane simultaneously. However, a car *cannot* just be "copied," whereas a song file that they could each listen to on these simultaneous trips *can* be. A car *design* could be copied just like a song file, but not an actual new instance of a car.

The point here is not to enter into the pros and cons of copyright legislation and entertainment business models,[27] but only to show relevant descriptive distinctions. A copy of a nonscarce good *can* be freely produced while a "copy" of a rival good such as a car *cannot* be made in this way. Either control of a given single instance of a car must be transferred (through sale, gift, or theft), or an entirely new instance of a car must be constructed from additional and different scarce instances of the requisite materials and energy.

Tucker and Kinsella's article set up a relevant binary along these lines:

> One helpful way to understand this is to classify all goods as either finite and therefore normally scarce or nonfinite and therefore naturally nonscarce...It is scarce goods that serve as means for action, while nonscarce goods **that can be copied without displacing the original** are not *means* but *guides* for action.
>
> ...[A] recipe can be shared unto infinity. Once the information in the recipe and the techniques of making it are released, they are free goods, nonscarce goods, or nonfinite goods.

Accordingly, a scarce good (in the property theory sense), or a rival good, is **a good that is *not* copiable with perfect remainder of the original and is *not* useable by multiple actors simultaneously without mutual interference.**

In the age of digital goods, nonscarce goods have proliferated and become much more significant to modern life. The category includes abstract goods such as ideas, text and music files, patterns, plans, recipes, methods, and so on. Specifically, it includes the *meaning and content* of all types of media, text, and other abstract and informational objects.

7. Bitcoin as a rival digital good

With bitcoin, matters are different. Although bitcoin units are part of the digital realm, they *cannot* by "copied," only transferred. Forked and altered new block chains (altcoins) can be created *ad infinitum*, but in no case are the resulting newly created units *bitcoin* units; they are units of the various altcoins instead.

[27] On which I recommend work done at *The Center for the Study of Innovative Freedom* (C4SIS.org) and *Techdirt* (techdirt.com).

Although bitcoin is information, the Bitcoin protocol and network simulate the properties of natural scarcity in the rival, property-theory sense, such that bitcoin can function in the social role of facilitating indirect-exchange transactions. It could not fill this role if it were an ordinary digital good, because such goods are in their descriptive natures nonscarce (nonrival) and could easily be copied and inflated into compounding superabundance and therefore uselessness in a trading role.

Each bitcoin unit can be associated with only one wallet at one time due to the protocol's methods of ubiquitously recording transactions and preventing double spending.[28] It is critical to understand that these qualities of bitcoin scarcity are not merely due to add-on security measures. They are not appended legal or technical protections. These qualities are *inseparable attributes* of bitcoin as it exists, and it exists in no sense other than as an integral attribute of the Bitcoin protocol and network.[29]

As should be clear by now, it is not necessary to fuss over objectivistic and context-shifting considerations such as whether an abstract collection of digits in certain configurations can "really" be a good or not. Böhm-Bawerk's insertion of the word "corporeal" into his 1881 sentence is not a separate criterion for something to serve as a means, a point much more easily seen today than over 130 years ago. Böhm-Bawerk nevertheless clearly explained that one must observe what people are *doing* to understand what goods *are*, an insight that Mises would later run with in his systematic action-based reconstruction of economic theory.

Bitcoin has brought *authentic* rival scarcity into the realm of digital goods. This is not the artificially imposed, legally constructed scarcity of intellectual property legislation. It is not a type of DRM system that attempts to use technical add-on measures to create artificial scarcity out of informational objects that are in their nature not otherwise scarce. The Bitcoin protocol has set up a type of scarcity that is inherent to and inseparable from the nature of the digital good itself.

A bitcoin unit viewed as an object of action also meets another essential criterion from Böhm-Bawerk—it can be exclusively controlled. As Campan explained:

---

[28] This is true for most ordinary transactions and sufficient for general understanding. However, as-yet rarely used transaction forms enable the release of funds only under certain more complex conditions. For example, spending a specified input can be set up to require not just one signature, but, say, two out of three signatures, or other specified conditions that can be built into more complex transactions. It is in reference to such possibilities that the term "programmable money" is sometimes used to describe bitcoin.

[29] For a technical description of how Bitcoin functions, see my video lecture *Bitcoin Decrypted Part II: Technical aspects* (December 2013). Part I also outlines an integral unit/system duality approach applied in a monetary context.

> It is necessary that the thing in question be disposable or available to us. We must possess the full power of disposal over it if we are really to command its power to satisfy our wants...the possession of a good cannot simply be decreed: either you possess effective control over it or not. (24)

The Bitcoin protocol achieves this through public key encryption, which allows effective control of bitcoin in a user's wallet, provided said user maintains control of signing keys and/or related passwords. Once a bitcoin unit is transferred from one wallet to another, it is no longer "in" the originating wallet, but exclusively "in" the destination wallet instead. A unit's state of address assignment is mutually exclusive to its being in some other state of address assignment at any given time, and this mutual exclusivity of assignment is a central element in the ontology of what a bitcoin unit *is*, as contrasted with something else that is *not* one.

Thus, in the rival, property-theory sense of scarcity, bitcoin qualifies, not as nonscarce like most other abstract or digital objects, but as scarce in the rival sense used in the foundations of property-theory reasoning. A given bitcoin unit is "**a good that is *not* copiable with perfect remainder of the original and is *not* useable by multiple actors simultaneously without mutual interference."**

Once a signing key to a Bitcoin address is copied, more than one party can have the key at the same time, as with any other nonscarce good. However, even so, only one party can succeed in using this key to make use of any given bitcoin unit associated with that address in any specific instance.[30]

Clarifying the concept of scarcity in both its economic-theory (object of action) and property-theory (rivalry) senses is useful to understanding bitcoin and better separating the concepts of scarcity and tangibility. For some observers, it was tangibility that had seemingly held together all the traditional money-commodity characteristics in the form of a solid coin of silver, gold, or copper. Upon seeing that bitcoin lacks tangibility, it seemed intuitively obvious that it must also lack, or at least be weak on, associated monetary characteristics such as durability and supply stability. We therefore turn to such characteristics to examine bitcoin directly in terms of each one.

8. Applying a commodity-money checklist

Hülsmann's essay "How to Use Methodological Individualism"[31] was on a different theme, but the following paragraph from it nevertheless contains a great deal of interest for our topic, all in one convenient location:

---

[30] Again assuming standard as opposed to multi-signature transactions for simplicity of presentation.

[31] Hülsmann. 27 July 2009. *Mises Daily.*

> Media of exchange become ever more generally accepted to the extent that they are objectively more suitable than their competitors **in arranging indirect exchanges**. Silver is more suitable as a medium of exchange than cherry cakes because it is **durable, divisible, malleable, homogeneous, and carries a great purchasing power per weight unit**. Market participants are likely to recognize this relative superiority in a process of learning and imitation, and eventually most of them will use silver to carry out their transactions. Hence, one can explain why the technique of indirect exchange is adopted on an individual level; and one can explain **why specific media of exchange become generally accepted** and thus gradually turn into money.

There is much of relevance here, but for now I will consider how bitcoin fares against silver coins on the same characteristics (plus stock stability):

Is bitcoin...

1. ***Durable?*** Perfectly. Abstract digital objects do not change. However, this is subject to recording and replication, substrate non-destruction, signing keys and passwords not being lost, etc.

2. ***Divisible?*** Effectively infinite. Maximum of 2.1×10^{15} (21 quadrillion) units ("satoshis") to be reached around 2140, with greater divisibility possible.

3. ***Malleable?*** Irrelevant; not material. However, units can be managed and traded in a variety of ways; block chain data can be saved on different types of media; and many possible implementations, mining software and hardware, and client wallets are possible, each within the same Bitcoin protocol.

4. ***Homogeneous?*** Perfectly. More homogeneous than possible with any conceivable physical material because the homogeneity is mathematical (by definition) rather than physical (by empirical measurement relative to a definition).[32]

5. ***Competitive on purchasing power per weight unit?*** Its purchasing power per weight unit is infinite. Intangible code patterns lack the characteristic of weight, rendering the slightest purchasing power infinite in per-weight terms. This counter-intuitive property of having infinite value per unit of weight may help explain how the units were able to gradually gain a trading value seemingly from nothing, starting from small fractions of a cent.[33]

6. Now add: ***Competitive on total stock stability?*** Quantitative growth and terminal maximum quantity and timing are determined

[32] This is a critical property that systematic coin tracking or marking could threaten to undermine. Countervailing measures and strategies to defend fungibility and financial privacy exist and are in ongoing development. These include, but are not limited to, coin mixing, coinjoin, merge avoidance, and the use of hierarchical-deterministic wallets to help avoid address reuse.

[33] See *On the origins of Bitcoin* for a detailed account of this historical sequence.

computationally; macro supply of bitcoin units (theoretically) not subject to human manipulation.

On this initial reading, bitcoin appears competitively superior to metallic coins on factors 2–5, whereas factors 1 and 6 are open to contingencies and technical debate. These two criteria require further investigation, but bitcoin also appears potentially competitive and possibly superior on them as well. These are questions for empirical observation, specialized technical knowledge in the relevant fields of cryptography and computer science, and entrepreneurial prediction and speculation about the course of the future—not for abstract economic theory as such.

This analysis suggests other points with regard to several of these characteristics. First, purchasing power per weight was a major impetus in the evolution of paper and account entry substitutes for precious-metal coin monies. Another problem with metallic coins was gradual wear from circulation, which would eventually give rise to weight variations—a loss of homogeneity resulting from imperfect durability. Bitcoin does not share these weaknesses.

Second, it is intuitive to interpret the commodity-money characteristic of durability as a mainly material one. On reflection, however, a temporal aspect is central to the concept of durability in that it refers to rates of change. To ask about durability is to ask the extent to which an object tends to change over time in certain of its properties under certain conditions. In the case of an abstract relationship on a network, it need not change at all. Although particular instances of recording substrates might degrade, the cryptographic data relationships on the block chain can be perfectly copied and copied again to new media, and it is in this sense that the durability of these data is potentially infinite for any conceivably relevant purpose.

Third, regarding divisibility, whereas fiat money issuers stand ready to add integers to paper fiat notes and phase out the smallest denominations of change to accommodate the steady loss of fiat-unit value; the Bitcoin protocol is capable of supporting divisibility to as many decimal places as are demanded to adjust to value gains over time. This is a diametric contrast the further implications of which would be difficult to overstate.

9. Comparative-realist versus imaginary-perfection methods

The ultimate potential for manipulation of the total bitcoin stock (factor 6 above) is a key question that is certainly a technical one, possibly with philosophical aspects. Can it be established that future quantitative supply manipulation at the macro level *cannot* occur? Would that require "proving" a technical and empirical negative?

Whatever the factors and answers, it is important to apply the realistic-comparative method in preference to the tempting imaginary-perfection method.

If one of the criteria required of a candidate for becoming a sound money is proof of a technical and empirical negative, then meeting such an impossible standard ought to be required equally of all candidates.

Applying the comparative-realist method to fiat monies, we know that large-scale, distortive, quantitative manipulation of the money supply can occur—and in all known cases *actually does*. Moreover, it strains credulity to imagine any conceivable fiat money system in which this would not be the case, since enabling just such manipulation was among the main founding purposes of such monetary central-planning schemes.

Likewise, concerning any proposed relaunch of a precious-metal currency, comparisons on hypotheticals would also have to be even-handed. The stock of precious metals adjusts over time with mine output and other factors. Nevertheless, at the extreme, can it be shown that cheap synthetic gold could *not ever be produced* (as the alchemists had dreamed), thereby collapsing the price of gold by inflating its supply (as the alchemists may not have thought through far enough)? Gold can already be synthesized in particle accelerators and nuclear reactors, just not *cheaply*.[34] Asteroid mining plans are already out of the science fiction books and on the engineering table. Moreover, any use of metallic money beyond a primitive and local level must rely on money substitutes—and all their proven and persistent vulnerabilities to degrading substitution rates—to boost divisibility and transferability. Bitcoin itself requires no such money substitutes to deliver these same features and conveniences directly to users. These features are already part of the good itself.

Empirical perfection never comes to pass. The comparative method must be recalled and put to use in the assessment of real alternatives; *relative* pros and cons must be assessed. Attempts to reject real options by comparing them with non-existent idealized versions of other options must themselves be rejected. Human action means choosing among alternatives. The Misesian tradition of economics is positioned as one part of the study of such action. The study of society is the study of acting persons joined in a grand, interacting process of trial and error writ large, and it is not only to Bitcoin and the multifaceted communities involved with it to which this characterization applies, but to every endeavor.

[34] en.wikipedia.org/wiki/Synthesis_of_precious_metals

References

Bastiat, Frédéric. 2007 [1850]. *The Law*. Auburn, Alabama: Mises Institute

Böhm-Bawerk, Eugen von. 1962 [1881]. “Whether Legal Rights and Relationships are Economic Goods.” *Shorter Classics of Eugen von Böhm-Bawerk*. South Holland, Illinois: Libertarian Press; originally, “Rechte und Verhältnisse vom Standpunkte der volkwirtschaftlichen Güterlehre.” Innsbruck, Austria: Verlag der Wagner’schen Universitäts-Buchhandlung.

Campan, Gael J. 1999. “Does Justice Qualify as an Economic Good?” *The Quarterly Journal of Austrian Economics.* 2, 1 (Spring): 21–33. mises.org/journals/qjae/pdf/Qjae212.pdf

Graf, Konrad. 2011. “Action-Based Jurisprudence: Praxeological Legal Theory in Relation to Economic Theory, Ethics, and Legal Practice,” *Libertarian Papers* 3, 19.

———. 20 February 2013. “Misesian action theory is an approach to social theory, not just economics.” *konradsgraf.com.*

———. 14 September 2013. “Bitcoin as medium of exchange now and unit of account later: The inverse of Koning’s medieval coins.” *konradsgraf.com.*

———. 23 October 2013. *On the origins of Bitcoin: Stages of monetary evolution.* konradsgraf.com.

———. 27 December 2013. “Bitcoin Decrypted: Part I: Introduction and overview; Part II: Technical aspects; Part III: Social theory aspects.” *konradsgraf.com/bitcoin-decrypted*

———. 27 February 2014. “MtGox fiasco highlights advantages of Bitcoin and damage from regulation.” *konradsgraf.com*

Hoppe, Hans-Hermann. 14 May 2009. “‘The yield from money held’ reconsidered.” *Mises Daily.* mises.org/daily/3449

———. 2010 [1989]. *A Theory of Socialism and Capitalism.* Auburn, Alabama: Mises Institute.

Hülsmann, Jörg Guido. 2003. “Facts and Counterfactuals in Economic Law.” *Journal of Libertarian Studies* 17 (1): 57–102.

———. 2003b. “From Value Theory to Praxeology,” Introduction to the third edition of *Epistemological Problems of Economics* by Ludwig von Mises. Auburn, Alabama: Mises Institute.

———. 2004. “The A Priori Foundations of Property Economics.” *The Quarterly Journal of Austrian Economics* 7 (4): 41–68. mises.org/journals/qjae/pdf/qjae7_4_4.pdf.

———. 2007. *Mises: The Last Knight of Liberalism.* Auburn, Alabama: Mises Institute. mises.org/document/3295/Mises-The-Last-Knight-of-Liberalism.

———. 2008. *The Ethics of Money Production.* Auburn, Alabama: Mises Institute. mises.org/document/3747/The-Ethics-of-Money-Production.

———. 27 July 2009. “How to Use Methodological Individualism.” *Mises Daily.* mises.org/daily/3578.

———. 2012. “The Early Evolution of Mises’s Monetary Thought,” *Theory of Money and Fiduciary Media: Essays in Celebration of the Centennial.* Auburn, Alabama: Mises Institute.

Kinsella, Stephan. 2001. “Against Intellectual Property.” *Journal of Libertarian Studies* 15 (2): 1–53. mises.org/document/3582.

Menger, Carl. *On the origins of money.* 2009 [1892]. Auburn, Alabama: Ludwig von Mises Institute. Translation by C. A. Foley.

Mises, Ludwig von. 1912. *Theorie des Geldes und der Umlaufsmittel*. Munchen und Leipzig: Ferlag von Duncker & Humblot. mises.org/document/3298/

———. 1940. *Nationalökonomie: Theorie des Handelns und Wirtschaftens.* Genf: Editions Union. mises.org/document/5371/Nationalokonomie-Theorie-des-Handelns-und-Wirtschaftens

———. 1953 [1912]. *The Theory of Money and* Credit. New Haven: Yale University Press. Reprinted and online: mises.org/document/194/The-Theory-of-Money-and-Credit

———. 1998 [1949]. *Human Action: A Treatise on Economics.* The Scholar’s Edition. Auburn, Alabama: Mises Institute. mises.org/document/3250

———. 2006 [1962]. *The Ultimate Foundation of Economic Science: An Essay on Method.* Indianapolis, IN: Liberty Fund

Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to Peer Electronic Cash System.” White Paper. bitcoin.org/bitcoin.pdf

Rothbard, Murray N. 2004 [1962, 1970]. *Man, Economy, and State, with Power and Market.* The Scholar’s Edition. Auburn, Alabama: Mises Institute. mises.org/rothbard/mes.asp

Šurda, Peter. 2012. *Economics of Bitcion: Is Bitcoin an alternative to fiat currencies and gold?* Thesis for the Vienna University of Economics and Business. dev.economicsofbitcoin.com/mastersthesis/mastersthesis-surda-2012-11-19b.pdf

———. 12 Mar 2013. “The classification and the future of Bitcoin,” *economicsofbitcoin.com.*

Tucker, Jeffrey A. and Stephan Kinsella. 25 August 2010. “Goods, Scarce and Nonscarce.” *Mises Daily*. mises.org/daily/4630/

New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market

Larissa Lee∗

Bitcoin is the first and most successful digital currency in the world. It polarizes the news almost daily, with either glowing reviews of the many benefits of an alternative and international currency, or doomsday predictions of anarchy, deflation, and another tulip bubble.

This article focuses on the truly innovative aspect of Bitcoin — and that which has gone mostly unnoticed since its inception — the technological platform used to transfer Bitcoin from one party to another. This technology is called the Blockchain. The Blockchain eschews a bank or other intermediary and allows parties to transfer funds directly to one another, using a peer-to-peer system. This disruptive technology has done for money transfers what email did for sending mail — by removing the need for a trusted third party just as email removed the need for using the post office to send mail.

If this technology can be used for peer-to-peer money transfers, why not extend the technology to accomplish other forms of transfers? Imagine selling a house or buying a car peer-to-peer. What about using the Blockchain technology to buy and sell stocks? Stocks exchanged completely peer-to-peer could resolve many of the issues facing the stock market today, including high frequency trading and short sales. This article develops a peer-to-peer stock market system, the legal implications of such a system, and how this system will fit in with current legislation and regulation.

∗ J.D., University of Utah S.J. Quinney College of Law; M.B.A., Boise State University. I wish to thank Professor Jeff Schwartz for his tireless advice, edits, and ideas; this article would not have been possible without his encouragement. I would also like to thank my husband, Denver Lee, for letting me harass him about cryptography and technology in general into the wee hours of the night. Finally, I am grateful for the hard work and input from the *Hastings Business Law Journal* staff.

I. INTRODUCTION

What do Lamborghinis, drug dealers, pirates, hackers, the Winklevoss twins, the FBI, and Congress have in common? Each has involved itself in some way in the phenomenon that is Bitcoin in the past few years. With a market capitalization of over $7 billion,[1] Bitcoin has garnered much attention, and not all of it is positive. Several countries have banned Bitcoin transfers altogether, while others — including the United States — have tried to place limits or restrictions on transfers by taxing those transfers. The European Union officially recognizes Bitcoin as a currency, but several other countries are grappling at how to classify it. Is it money? Property? A security? Hundreds of other digital currencies ("cryptocurrencies") have since popped up and it is still unclear what effect these will have on the global economy.

However, the truly innovative aspect of Bitcoin — and that which has gone mostly unnoticed since its inception — is the technological platform used to transfer Bitcoin from one party to another. This technology is called the Blockchain. The Blockchain eschews a bank or other intermediary and allows parties to transfer funds directly to one another, using a peer-to-peer system. This disruptive technology has done for money transfers what email did for sending mail — by removing the need for a trusted third party just as email removed the need for using the post office to send mail.

What about other practical implications of the Blockchain? Could this technology be extended beyond money transfers to accomplish other forms of transfers? Imagine selling a house or buying a car peer-to-peer. What about using the Blockchain technology to buy and sell stocks?[2] Stocks exchanged completely peer-to-peer ("cryptosecurities") could resolve many of the issues facing the stock market today, including high frequency trading and short sales.

This article seeks to develop and analyze these claims and examine

---

1. *Crypto-Currency Market Capitalizations*, COINMARKETCAP, http://coinmarketcap.com (last visited Apr. 26, 2016).

2. This idea was initially proposed in 2014 by Patrick Byrne, Chief Executive Officer of Overstock. Cade Metz, *Overstock's Radical Plan to Reinvent the Stock Market with Bitcoin*, WIRED (July 30, 2014, 6:30 AM), http://www.wired.com/2014/07/overstock-and-cryptocurrency/. Overstock tested this concept out with a $25 million private corporate "cryptobond" in June 2015. Josh Beckerman, *Overstock Launches Corporate Bond Billed as World's First Cryptocurrency*, WALL ST. J. (June 5, 2015, 8:03 PM), http://www.wsj.com/articles/overstock-launches-corporate-bond-billed-as-worlds-first-cryptosecurity-1433549038. In August 2015, Overstock announced the arrival of t0 (pronounced tee-zero), the world's first "Blockchain-based private and public equities trading platform." Pete Rizzo, *Overstock Unveils Blockchain Trading Platform at Nasdaq Event*, COINDESK (Aug. 5, 2015, 2:19 AM), http://www.coin desk.com/overstock-unveils-blockchain-trading-platform-to/.

other potential benefits and disadvantages of a peer-to-peer stock market system. Considering all of these factors, the article then looks at the legal implications of a cryptosecurities market and whether this market could fit within the existing legal regime, or whether Congress and the SEC would need to change the laws to fit the new system. This cryptosecurities market would be an alternative trading market, not a replacement for the current stock market regime.

The article proceeds in five parts. Part II examines the role of Bitcoin in today's society. Part III delves into the Blockchain, focusing on how this Bitcoin technology actually works and the process behind each Bitcoin transfer. Part IV examines the problems facing the current stock market regime and explores how a cryptosecurities market could correct these problems. Part V looks at the benefits and disadvantages of a peer-to-peer stock exchange. Finally, Part VI determines whether this new system of cryptosecurities could fit within existing laws and regulations, or whether new laws and regulations would need to be developed around this new technology.

II. WHAT IS BITCOIN?

The Bitcoin concept first emerged in October 2008 when Satoshi Nakamoto — a pseudonym for a person or possibly a group of people — published a whitepaper outlining the idea.[3] This paper envisioned a "purely peer-to-peer version of electronic cash" that would allow "online payments to be sent directly from one party to another without going through a financial institution."[4] Since this time, almost 700 other digital currencies have appeared with varying levels of success.[5] Although the focus of this article will be on Bitcoin's underlying technology and not Bitcoin itself, it is helpful to understand Bitcoin's impact on society, the government's attempt to define Bitcoin, and how Bitcoin gets its value.

A. BITCOIN'S IMPACT ON SOCIETY

For the first few years of its existence, Bitcoin yearned for legitimacy, but was used mainly for black market goods and illegal drugs sold over the internet.[6] Silk Road, the now-defunct illegal drug website, ran by a man

3. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (Oct. 2008), http://bitcoin.org/bitcoin.pdf.

4. *Id.*

5. *Crypto-Currency*, *supra* note 1.

6. *An Abridged History of Bitcoin*, N.Y. TIMES, http://www.ny times.com/interactive/technology /bitcoin-timeline.html?_r=0#/#time284_8158 (last updated Nov. 19, 2013).

calling himself The Dread Pirate Roberts, required users to buy and sell exclusively in Bitcoin in order to evade government authorities.[7] The site also used an eBay style escrow system that "consisted of an internal Bitcoin 'bank,' where every Silk Road user had to hold an account maintained by Silk Road, pending completion of the transaction."[8] It was not until late 2013 that the FBI finally shut down the online drug marketplace and began prosecuting Ross Ulbricht, who in February 2015, was convicted of narcotics and money laundering conspiracies using the alias The Dread Pirate Roberts.[9]

On November 18, 2013, the Senate held a hearing during the aftermath of the Silk Road shut down.[10] While regulators acknowledged that Bitcoins may be used for illicit purposes, they argued that Bitcoins are also "an innovative way of driving legitimate operations."[11] Overall, the tone of the hearing was optimistic. "The Senate hearing is the clearest indication yet of the government's desire to grapple with the consequences of [Bitcoin's] growth, and the recognition that Bitcoin and other similar networks could become more lasting and significant parts of the financial landscape."[12]

Today Bitcoins have been used to purchase various items such as a Lamborghini[13] and college tuition.[14] Bitcoin ATMs are currently popping up all around the globe.[15] Over 80,000 merchants currently accept Bitcoin

7. "The Dread Pirate Roberts isn't shy about naming Silk Road's active ingredient: The cryptographic digital currency known as Bitcoin. 'We've won the State's War on Drugs because of Bitcoin,' [Roberts] writes." Andy Greenberg, *Meet The Dread Pirate Roberts, The Man Behind Booming Black Market Drug Website Silk Road*, FORBES (Aug. 14, 2013, 11:31 AM), http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/.

8. Press Release, U.S. Dep't of Just., Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of Silk Road Website (Oct. 25, 2013), http://www.justice.gov/usao/nys/pressreleases/October13/SilkRoadSeizurePR.php?print=1.

9. Robert McMillan, *Who Owns the World's Biggest Bitcoin Wallet? The FBI*, WIRED (Dec. 18, 2013, 6:30 AM), http://www.wired.com/wiredenterprise/2013/12/fbi_wallet/; http://www.wired.com/2015/02/silk-road-ross-ulbricht-verdict/.

10. Cade Metz, *The Magic Number: Bitcoin Prices Top $1,000*, WIRED (Nov. 27, 2013, 10:59 AM), http://www.wired.com/business/2013/11/bitcoin-one-thousand/?cid=15030794.

11. *Id*.

12. *An Abridged History of Bitcoin*, *supra* note 6.

13. Craig Trudell, *Bitcoin Meets Tesla with Lamborghini Dealership's Model S Sale*, BLOOMBERG TECH. (Dec. 6, 2013, 10:00 PM), http://www.bloomberg.com/news/2013-12-06/bitcoin-meets-tesla-in-california-dealership-model-s-transaction.html.

14. Not only can you pay college tuition, but at a university in Cyprus, you can also get a master's degree in Digital Currency. Panos Mourdoukoutas, *Bitcoin Gets an Endorsement for College Tuition Payments and a MOOC*, FORBES (Nov. 21, 2013, 1:58 PM), http://www.forbes.com/sites/panosmourdoukoutas/2013/11/21/bitcoin-gets-an-endorsement-for-college-tuition-payments-and-a-mooc/.

15. Brian P. Eha, *Bitcoin ATMs are Spreading Across the World*, ENTREPRENEUR (Dec. 30, 2013, 5:20 PM), http://www.entrepreneur.com/article/230589.

payments.[16] Some of the major retailers that accept Bitcoin payments include Amazon, Microsoft, Home Depot, Target, Time, Inc., and — not surprisingly — Overstock.[17] Bitcoins have been pooled into investment trusts by online platforms such as SecondMarket where investors are able to "buy a stake in the Bitcoin market without directly purchasing the currency themselves."[18] Even the Winklevoss twins[19] have purchased a stake worth almost $11 million in Bitcoins and have filed paperwork with the Securities and Exchange Commission to create an exchange-traded fund, using only Bitcoins.[20] A federal district court in Texas declared these types of Bitcoin investments to be securities governed by SEC regulations.[21]

Some countries have formally recognized Bitcoin as a legitimate currency, while others have banned Bitcoin entirely.[22] Several countries have not banned Bitcoins but have issued clear warnings about the risks of Bitcoin use.[23] Not only is the enormous amount of volatility a big risk, but hacking into online Bitcoin wallets can also be a serious risk. For example, in October 2013, hackers stole $1.2 million from a company storing Bitcoins online.[24]

---

16. Greg Bensinger, *First U.S. Bitcoin Exchange Set to Open*, WALL ST. J. (Jan. 25, 2015), http://www.wsj.com/articles/first-u-s-bitcoin-exchange-set-to-open-1422221641.

17. Jonas Chokun, *Who Accepts Bitcoins as Payment? List of Companies, Stores, Shops*, BITCOIN VALUES, http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html (last visited May 24, 2015).

18. Brian P. Eha, *SecondMarket Establishes New Bitcoin Trust for Accredited Investors*, ENTREPRENEUR (Sept. 26, 2013), http://www.entrepreneur.com/article/228597.

19. Tyler and Cameron Winklevoss — most known for their legal battle with Mark Zuckerberg over the ownership of Facebook — launched Gemini in January 2015, the second U.S.-based Bitcoin exchange. Nathaniel Popper & Peter Lattman, *Never Mind Facebook; Winklevoss Twins Rule in Digital Money*, N.Y. TIMES (Apr. 11, 2013, 3:11 PM), http://dealbook.nytimes.com/2013/04/11/as-big-investors-emerge-bitcoin-gets-ready-for-its-close-up/?_r=0; Joanna Campione, *Bitcoin Comes to America: Now, with Regulated Exchange*, YAHOO FINANCE (May 7, 2015, 12:21 PM), http://finance.yahoo.com/news/first-bitcoin-exchange-gets-approval-from-new-york-state-regulators-022427666.html.

20. *An Abridged History of Bitcoin*, s*upra* note 6.

21. SEC v. Shavers et al., No. 4:13-CV-416**,** 2013 WL 4028182 (E.D. Texas, Aug. 6, 2013).

22. Germany and Canada both recognize Bitcoin as legal tender. Matt Clinch, *Bitcoin Recognized by Germany as 'Private Money'*, CNBC (Aug. 19, 2013, 10:25 AM), http://www.cnbc.com/id/100971898; Drew Hasselback, *Governments Ponder Legitimacy of Bitcoins*, FINANCIAL POST (Nov. 19, 2013, 4:52 PM), http://business.financialpost.com/2013/11/19/governments-ponder-legitimac y-of-bitcoins/. Countries banning Bitcoin include Thailand and China. Matt Clinch, *Bitcoin Banned in Thailand*, CNBC (July 30, 2013, 6:20 AM), http://www.cnbc.com/id/100923551; Andrew Mouton, *What a Bitcoin is Really Worth in India and China*, MARKET WATCH (Jan. 1, 2014, 7:02 AM), http://www.marketwatch.com/story/what-a-bitcoin-is-really-worth-in-india-and-china-2014-01-01.

23. While India has not banned Bitcoins outright, it has issued a warning on the dangers of Bitcoin use. Andrew Mouton, *What a Bitcoin is Really Worth in India and China*, MARKET WATCH (Jan. 1, 2014, 7:02 AM), http://www.marketwatch.com/story/what-a-bitcoin-is-really-worth-in-india-and-china-2014-01-01. France has issued similar warnings. Robin Sidel et al., *Central Banks Warn of Bitcoin Risks*, WALL ST. J. (Dec. 5, 2013, 11:23 PM), http://online.wsj.com/news/articles/SB100014240527023034978045792394512974248 42.

24. Robert McMillan, *$1.2M Hack Shows Why You Should Never Store Bitcoins on the Internet*,

Many Bitcoin critics and those wishing to regulate or abolish Bitcoin point out its propensity to be used in facilitating illegal transactions. Bitcoin transfers are completely anonymous, and extremely difficult to trace. However, almost all of these issues also occur when parties to a transaction use cash. Cash is extremely difficult to trace, and most transactions are anonymous. The one distinguishable trait is that Bitcoin can be used to make payments online whereas cash cannot be used online. This enables more illicit uses of the currency because even the parties buying and selling can remain anonymous with almost no information about each other.[25] When exchanging cash, the parties must at least determine how and where to exchange the cash for the illicit goods.

B. What is a Bitcoin — Currency, Property, or Security?

Although Satoshi Nakamoto referred to Bitcoin as "electronic cash," no one is really sure yet what Bitcoins are. Bitcoins do not have a physical form, and although there are several options of novelty coins one can purchase, the actual Bitcoin itself is just a unique string of numbers that only the holder of the Bitcoin has access to. Additionally, like all other digital currency, Bitcoin is not considered legal tender in any country.

By 2014, with millions of dollars in Bitcoin being exchanged tax-free every hour, the Internal Revenue Service ("IRS") classified Bitcoin and all other digital currencies as property for tax purposes, as opposed to as currency.[26] This decision encourages investment in Bitcoin while discouraging users to trade in Bitcoin because they must calculate gain or loss and report it like they would for any other property for tax purposes. However, stocks and bonds are also classified as property for tax purposes and therefore if Bitcoins are more like a security and less like a currency then it makes sense to classify them as property.

In the Securities Act of 1933, Congress defined a "security" as:

> any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing

WIRED (Nov. 7, 2013, 3:49 PM), http://www.wired.com/wiredenterprise/2013/11/inputs/.

25. Although transactions are completed anonymously, it might be possible to track a user's identity by following the Bitcoin through the Blockchain and to a Bitcoin exchange, and then subpoenaing the exchange. Tom Simonite, *Mapping the Bitcoin Economy Could Reveal Users' Identities*, MIT TECH. REV. (Sept. 5, 2013), http://www.technologyreview.com/news/518816/mapping-the-bitcoin-economy-could-reveal-users-identities/.

26. Josh Ungerman, *IRS Approach to Taxation of Bitcoin*, FORBES (Dec. 4, 2014, 1:02 AM), http://www.forbes.com/sites/irswatch/2014/12/04/irs-approach-to-taxation-of-bitcoin/.

> agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, factional undivided interest in oil, gas, or other mineral rights, and put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.[27]

The U.S. Supreme Court in *Marine Bank v. Weaver*[28] held that the definition of a security is meant to be broad and includes not only stocks and bonds but also the "countless and variable schemes devised by those who seek the use of the money of others on the promise of profits."[29] It is unlikely that Bitcoin, unattached to any investment trust or other scheme, falls into this definition.

First, cryptocurrencies — or any currencies for that matter — are not explicitly listed in the statute. Second, Bitcoin does not pass the investment contract test the U.S. Supreme Court developed in *SEC v. W.J. Howey Co*. (the "*Howey* test").[30] For an investment to constitute a security under the *Howey* test, it must involve the investment of money — or any valuable consideration — in a common enterprise with a reasonable expectation of profits derived primarily from the efforts of a promoter or third party.[31]

The first issue is that there is no common enterprise. Unless attached to an investment trust, Bitcoins are not being pooled into groups. No one enterprise is in charge of Bitcoin, seeking to take people's money with the promise of profits. Bitcoin is purely autonomous and has no central authority. Secondly, "primarily from the efforts of another" prong is not satisfied in the case of Bitcoin because whether the value of Bitcoin rises or falls is not dependent on anyone's efforts — the change in price is based on

27. 15 U.S.C. § 77(b)(a)(1) (2012).
28. Marine Bank v. Weaver, 455 U.S. 551 (1982).
29. *Id.* at 555.
30. SEC v. W.J. Howey Co., 328 U.S. 293 (1946).
31. *Id.* at 298–99. *Howey* originally said *solely* from the efforts of others instead of primarily, but the courts have since modified this test.

fluctuations in value tied to market conditions. Additionally, Bitcoin on its own does not pay out dividends, and voting rights are not in proportion to the number of Bitcoins owned, but rather the amount of computational power a user devotes to the system.[32]

The other issue with declaring all Bitcoins to be securities is that there is no issuer — just users trading amongst themselves. "The fundamental principle underlying the 1933 Act is that all offers and sales of securities require . . . [issuer] registration unless an exemption is available."[33] Because there is no issuer and it would be impossible to register Bitcoin as a security, it is unlikely it could be classified as a security, outside of being pooled into an investment trust of some kind. Although the jury is still out on what a Bitcoin is, for purposes of this article I will refer to it as a digital currency.[34]

C. HOW DO BITCOINS GET THEIR VALUE?

Many wonder how Bitcoin and other alternative currencies get their value. It is difficult to imagine how a single Bitcoin could be worth hundreds or even thousands of U.S. dollars. Many have claimed that Bitcoin is no more than a Ponzi scheme,[35] or have worried that it represents the next tulip disaster waiting to happen.[36] However, most of the same arguments could be made about the U.S. dollar. For most of the greenback's history, the value of the dollar was tied to the government's

32. For Bitcoin, "voting rights" are essentially given to the Bitcoin miners. This concept is explored more in the following section.

33. JAMES M. BARTOS, UNITED STATES SECURITIES LAW: A PRACTICAL GUIDE, 8 (3rd ed. 2006) (emphasis omitted).

34. Notably, the European Union recently declared Bitcoin a "currency" and not "property" for tax purposes, meaning transfers of Bitcoin in the EU will not be considered a taxable event. *See* Sam Schechner, *EU Rules Bitcoin is a Currency, Not a Commodity — Virtually*, WALL ST. J. (Oct. 22, 2015, 6:15 AM), http://blogs.wsj.com/digits/2015/10/22/eu-rules-bitcoin-is-a-currency-not-a-commodity-virtually/.

35. Eric Posner, *Fool's Gold: Bitcoin is a Ponzi Scheme — the Internet's Favorite Currency Will Collapse*, SLATE (April 11, 2013, 11:11 AM), www.slate.com/articles/news_and_politics/view_from_chicago/2013/04/bitcoin_is_a_ponzi_scheme_the_internet_currency_will_collapse.html; Matt O'Brien, *Bitcoin Revealed: a Ponzi Scheme for Redistributing Wealth from One Libertarian to Another*, THE WASH. POST (Jan. 14, 2015), http://www.washingtonpost.com/blogs/wonkblog/wp/2015/01/14 /bitcoin-is-revealed-a-ponzi-scheme-for-redistributing-wealth-from-one-libertarian-to-another/; Bruce Richards, *Bitcoin a Ponzi Scheme, Fraud: Marathon's Richards*, BLOOMBERG BUSINESS (Feb. 25, 2014), http://www.bloomberg.com/news/videos/b/c6454137-4042-4d83-a1e4-ed77253b7652. *Compare with* Andy Bay, *Bitcoin is Not a Ponzi Scheme*, TED (Mar. 18, 2014), http://www.ted.com/conversations/23415/bitcoin_is_not_a_ponzi_scheme.html; Evander Smart, *World Bank: Bitcoin is Not a Ponzi Scheme*, CRYPTOCOINS NEWS (Nov. 19, 2014), https://www.cryptocoinsnews.com/world-bank-bitcoin-not-ponzi-scheme/.

36. *See* Charles Mackey's chapter on the "Tulipomania" that occurred among the Dutch in the 17th century. CHARLES MACKAY, EXTRAORDINARY POPULAR DELUSIONS AND THE MADNESS OF CROWDS, 89–97 (2d ed. 1890).

guarantee that you could trade in your dollars at any time for gold or silver.[37] In 1971, the U.S. abandoned the gold standard and now its value is backed solely by the Federal Reserve and the confidence of the American people.[38]

Bitcoin, too, is backed by the confidence of its users. Bitcoin users prefer Bitcoin to traditional currency for several reasons. In describing its purpose, a digital currency called Bitshares posted the following to its website:

> Today many people have lost faith in the financial institutions we've trusted for centuries. Some of our largest banks have failed and no longer exist. Those that survived needed massive bailouts. Citizens in some countries have lost their life savings to pay for failed government decisions. And for those who do find safety, the value of their savings is being drained by the constant drip of inflation. Our financial system is overdue for a reset.[39]

As you may have surmised from the above quote, the number one reason why users are attracted to Bitcoin is mistrust of the government and its centralized federal reserve. Many economists are concerned with the government's ability to print new money whenever it wants, which causes inflation. The total number of Bitcoins, on the other hand, is permanently fixed at 21 million coins. Bitcoin users also like the fact that the transactions are made and controlled by the people, with complete transparency and a record of every Bitcoin transaction available to anyone who wishes to view it.

Other advantages of Bitcoin include: the ability to send or receive money at any time of day or night, including weekends and holidays; lower transaction fees than what are charged by banks and credit card companies;[40] low risk of fraud for merchants since transactions are irreversible; and the transparent nature of the Blockchain.[41]

That said, confidence in Bitcoin due mainly to external events has

37. Brian Domitrovic, *Aug. 15, 1971: A Date Which Has Lived in Infamy*, FORBES (Aug. 14, 2011, 7:36 PM), http://www.forbes.com/sites/briandomitrovic/2011/08/14/august-15-1971-a-date-which-has-lived-in-infamy/.

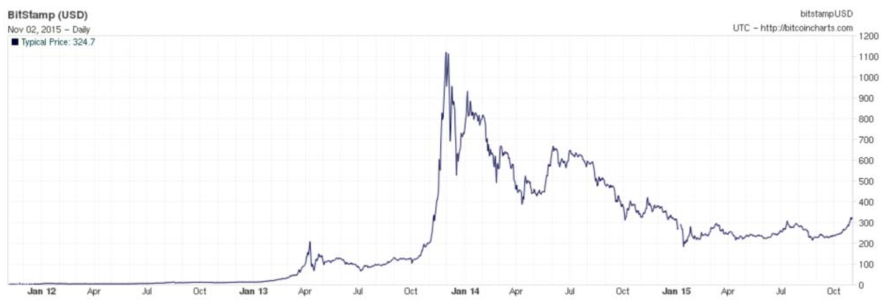
38. *Id.*

39. ABOUT BITSHARES, http://bitshares-x.info/about.php (last visited Dec. 1, 2014).

40. "While credit card networks charge merchants fees in the range of 3 to 4 percent of the total amount of a transaction, and the average cost of international remittances is 8.5 percent, a Bitcoin transaction can cost less than 1 percent." Jerry Brito et al., *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 26 COLUM. SCI. & TECH. L. REV. 144, 150 (2014).

41. *What are the Advantages of Bitcoin?*, BITCOIN: FREQUENTLY ASKED QUESTIONS, https://bitcoin.org/en/faq#what-are-the-advantages-of-bitcoin (last visited May 24, 2015).

created a lot of volatility in the currency in the past few years. The first Bitcoin transaction occurred in 2009, but it was not until February 2011 that Bitcoin's value matched the value of the U.S. Dollar.[42] At the start of 2013, a single Bitcoin was worth $13. A year later, Bitcoins were selling for around $900.[43] By December 2014, Bitcoins were selling for around $400.[44] At its peak in December 2013, a single Bitcoin was worth $1,145.[45] The volatility has greatly decreased in the past year with the average price of a Bitcoin staying right around $300.[46]



This Chart shows the value of one Bitcoin from 2011-2015.[47]

III. BITCOIN'S TECHNOLOGY — THE BLOCKCHAIN

Bitcoin is a digital currency. Unlike traditional currency and coin, Bitcoin does not have a physical form. This means that Bitcoins are stored, transferred, bought, and sold completely online, using the Blockchain. These transactions can be performed completely peer-to-peer, meaning without the assistance and verification of a trusted third party (such as a bank). Additionally, Bitcoin users can go through an exchange to complete this process for them. Either way, the technology behind the Bitcoin transfers is the same.

This section first provides an introduction to the Blockchain and its unique characteristics, including transparency, decentralization, mining, and use of cryptography. Second, the section walks through an example of

42. Loz Blain, *The Rise of Bitcoin: Bonanza or Bust?*, GIZMAG (Feb. 19, 2013), http://www.gizmag.com/bitcoin-creation-value-overview/26325/.

43. The values represent Bitcoin purchases in Salt Lake City as of January 2, 2014. BITCOIN CHARTS, http://bitcoincharts.com (last visited Jan. 2, 2014).

44. *Id.*

45. Michael J. Casey, *Bitcoin Trading Platform Atlas Partners with National Stock Exchange*, WALL ST. J. (Apr. 23, 2014, 12:16 AM), http://www.wsj.com/articles/SB10001424052702304049904579518224044905190.

46. The average Bitcoin sold for $325 in 2015. BITCOIN CHARTS, *supra* note 43.

47. *Bitstamp (USD)*, BITCOIN CHARTS, http://bitcoincharts.com/charts/bitstampUSD#rg1460ztgTzx (last visited Nov. 1, 2015).

how a peer-to-peer transaction works on the Blockchain, from the individual transaction level to incorporating the transaction into the Blockchain to completing the proof necessary to ensure the transaction's validity. Third, the section looks at some of the concerns associated with the proof stage of the Blockchain and some of the alternatives to this system. Finally, the section explains how the Blockchain could be implemented for peer-to-peer stock trading on a cryptosecurities market.

A. The ABCs of the Blockchain

1. Transparency and Anonymity

The Blockchain acts as a public ledger or transaction database and allows any person who downloads the Bitcoin software onto his or her computer to view a complete history of every Bitcoin transaction ever completed. This ledger may also be viewed online at Blockchain.info. Each individual Bitcoin may be traced from its inception to present day.

While the transactions are entirely transparent, the identity of the users conducting the transactions is more difficult to determine. Although many Bitcoin users operate under the assumption that the Blockchain allows for anonymous transfers — see, e.g., Ross Ulbricht of Silk Road[48] — the reality is that, while the identity of the users is difficult to trace, it is still possible to trace user identity through a variety of different methods, including tracking IP addresses.[49]

2. Decentralization

The Blockchain does not have a central bank, a CEO, intermediary, or anyone else in charge. Like Wikipedia, Craigslist, and the ocean starfish that cling to rocky shorelines,[50] the Blockchain is completely decentralized.

48. On February 4, 2015, Ross Ulbricht was convicted of creating the black market illegal drug website Silk Road. Ulbricht operated under the assumption that his dealings were private, however Ulbricht "misplaced trust in a handful of technologies" and the FBI was able to trace Ulbricht as the Dread Pirate Roberts. Joab Jackson, *5 Technologies That Betrayed Silk Road's Anonymity*, PCWORLD (Feb. 9, 2015, 2:36 PM), http://www.pcworld.com/article/2881772/four-technologies-that-betrayed-silk-roads-anonymity.html. Ironically, eighteen months after the Silk Road shutdown, two federal agents involved in taking down the site and Ulbricht were arrested for stealing millions of dollars of Silk Road money and depositing it into their own personal accounts, believing that anonymity would protect these illegal transfers. Andy Greenberg, *DEA Agent Charged with Acting as a Paid Mole for Silk Road*, WIRED (Mar. 30, 2015, 1:40 PM), http://www.wired.com/2015/03/dea-agent-charged-acting-paid-mole-silk-road/.

49. Alex Biryokov et al., *Deanonymisation of Clients in Bitcoin P2P Network* (Nov. 2014), http://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf.

50. Much like the Blockchain, "the starfish doesn't have a head. Its central body isn't even in charge. In fact, the major organs are replicated throughout each and every arm. If you cut the starfish

Any person in the world with an internet connection can download the software and will have access to what everyone else within the system has, including the ability to mine Bitcoin. This design was not by accident; "indeed the lack of such centripetal features was a core design goal for Bitcoin; as Nakamoto once wrote, '[a]t some point I became convinced there was a way to do this without any trust required at all and couldn't resist to keep thinking about it.'"[51]

An advantage of this type of decentralized financial system is that it cannot be censored. "For example, while PayPal froze the accounts of WikiLeaks after it released secret State Department cables, and prevented its customers from making donations to the group, such transactional prior restraint would not be possible on the Bitcoin network because there is no intermediary."[52]

Any other financial exchange system before Bitcoin required trust — in the form of a trusted third party that verifies each transaction. Rather than trust, the Blockchain relies on "proof" to determine if a transaction is authentic.[53] This proof allows the system to operate autonomously, with each user looking out for its own best interest and, in the process, keeping the entire system honest and secure. For Bitcoin, the proof is established through use of computational power ("CPU"). The users that devote the most CPU are able to prove that the transaction is accurate and authentic. This proof is discussed further in the Proof-of-Work section *infra*.

3. Mining

The Blockchain is managed by people called "miners" or "nodes." The miners keep the system running and ensure double transactions are not taking place and that each transaction is legitimate. As Bitcoin transactions become more complex, miners are increasingly working in teams rather than individually to more quickly solve the computational problem. The amount of CPU miners put into a given transaction works effectively as a vote, where the transaction that devotes the most CPU or votes wins and gets added to the chain.

in half, you'll be in for a surprise: the animal won't die, and pretty soon you'll have two starfish to deal with." ORI BRAFMAN & ROD BECKSTROM, THE STARFISH AND THE SPIDER 35 (2006).

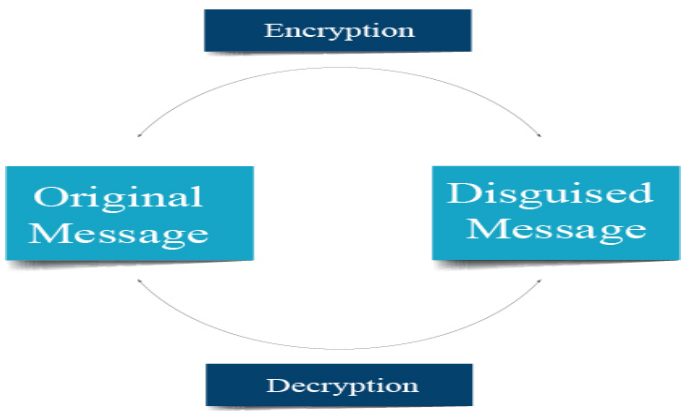
51. Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. U. L. REV. ONLINE 257, 259–60 (2014) (quoting Satoshi Nakamoto, *Re: Transactions and Scripts: DUP HASH160 ... EQUALVERIFY CHECKSIG*, BITCOIN FORUM (June 18, 2010, 4:17 PM), https://bitcointalk.org/index.php?topic=195.msg1617#msg1617).

52. Brito et al., *supra* note 40, at 149.

53. *See infra* Section III.C for a discussion on the "proof-of-work" method.

4. *Cryptography*

The Blockchain uses cryptography to secure its transactions. Cryptography is "the art of creating and using methods of disguising messages, using codes, ciphers, and other methods, so that only certain people can see the real message."[54] Cryptography is derived from the Greek words *kryptos* (hidden) and *graphein* (writing).[55] If Alice wants to send Bob a secret message using cryptography, Alice would *encrypt* the message which would convert the original message into a disguised message, and then Bob would *decrypt* the message to convert the disguised message back into the original message.[56]



Cryptography can range from very simple to extremely complex. Probably the simplest way to send a cryptographic message is to merely rearrange the letters in a message. Julius Caesar used a simple form of cryptography to send messages to his generals by replacing each letter in a word with a letter three positions down in the alphabet (e.g. a=d, m=p).[57] This is called the Caesar Cipher.[58]

One type of cryptography that Bitcoin employs is called SHA-256. This type of cryptography is one way, meaning the disguised message can never be encrypted back to the original message. For example, if Alice wants to send Bob a love letter using SHA-256, she will start with her

54. A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 713 (1995).

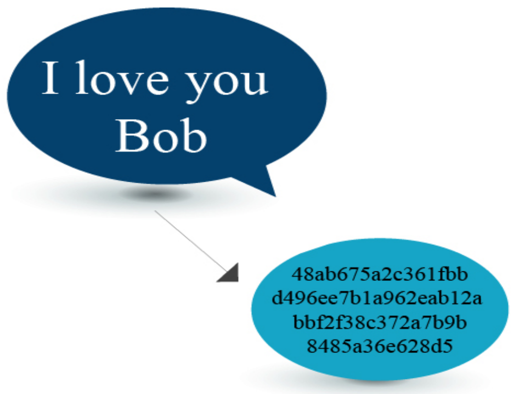
55. Monica Pawlan, *Cryptography: The Ancient Art of Secret Messages* (Feb. 1998), http://www.pawlan.com/monica/articles/crypto/.

56. Froomkin, *supra* note 54, at 714.

57. *Caesar Cipher*, PRACTICAL CRYPTOGRAPHY, http://practicalcryptography.com/ciphers/caesar-cipher/.

58. *Id.*

original message, which can be of any arbitrary length. If she puts "I love you Bob" through SHA-256, the encrypted message is called a "hash" and will always be exactly 64 numbers and characters in length.[59] In this case, the disguised message/hash is: 48ab675a2c361fbbd496ee7b1a962eab12a bbf2f38c372a7b9b8485a36e628d5.



If the only information you have is this hash or disguised message, it is impossible to know that the original message was "I love you Bob." However, if you know the input is "I love you Bob," you can easily put it through the SHA-256 converter and will always end up with the same resulting hash. If, however, you change *anything* in the original message including punctuation or capitalization, the result is a completely different hash. For example, "I lov you Bob" becomes: d63ea03682f1849bfc1c8 76fad349c44207cfb77935720dbef1e8adbf64f2d15. To understand how cryptography fits into the Blockchain, I will walk through a step-by-step example of a Bitcoin transaction.

B. AN EXAMPLE OF HOW TRANSACTIONS ARE PROCESSED AND INCORPORATED ON THE BLOCKCHAIN — THE STORY OF ALICE AND BOB

To understand how these transactions work and fit in to the Blockchain, it is easiest to start at the micro level and then expand to the macro level.[60] This section first discusses what goes on at the individual transaction level, then how the transactions are incorporated into the blocks

59. Calculate your own SHA-256 hashes at *Calculate a SHA hash with 256 bits*, ONLINE-CONVERT.COM, http://hash.online-convert.com/sha256-generator (last visited Apr. 10, 2016).

60. This is a very high level summary of how this technology works. For an excellent and greatly detailed explanation of the minutiae of these transactions, see ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN (2014).

on the Blockchain, and then how proof-of-work keeps the blocks in order and prevents double spending.

1. The Transaction — Alice Buys a Pizza

Most of the transactional steps below are accomplished automatically through software programs and users rarely know this level of detail about their Bitcoins. However, it is helpful to know the process of these transactions to better understand how this same technology could be used in a cryptosecurities market.

a. Step 1 – The Bitcoin Wallet

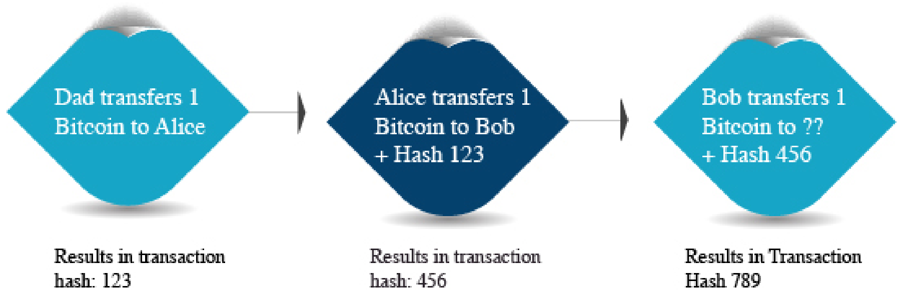
Let's say Alice wants to buy a pizza from Bob using Bitcoin.[61] If Alice were using cash, she would reach into her back pocket or purse and pull out her wallet, select the desired amount of cash, and then give the cash to Bob. Since Alice wants to pay with Bitcoin, she will go into her *Bitcoin wallet* — stored either on her computer or online — which holds all of Alice's Bitcoins.

b. Step 2 – The Message

Alice will then create a message to the effect of "I want to transfer one Bitcoin to Bob."[62] The message will also include a "hash" from the last time this Bitcoin was used. For example, say Alice's dad gave Alice the Bitcoin for her birthday. The transaction between Alice and her dad results in a digest or transaction hash. This hash is used as part of her message in the Alice-Bob transaction. Once the Alice-Bob transaction is complete, it will create a new hash that will be used when Bob is ready to transfer his Bitcoin to someone else. This is how it is possible to track each Bitcoin all the back to its inception. The illustraction below is a representation of this example.

61. A lot of the information from this example comes from: *Bitcoin: Transaction Records*, KHAN ACADEMY, https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-transaction-records (last visited Mar. 15, 2016).

62. For simplicity's sake, I will use one Bitcoin for this example, although that would be an incredibly expensive pizza. Also, the very first thing ever purchased with Bitcoin was a pizza, so it is fitting.



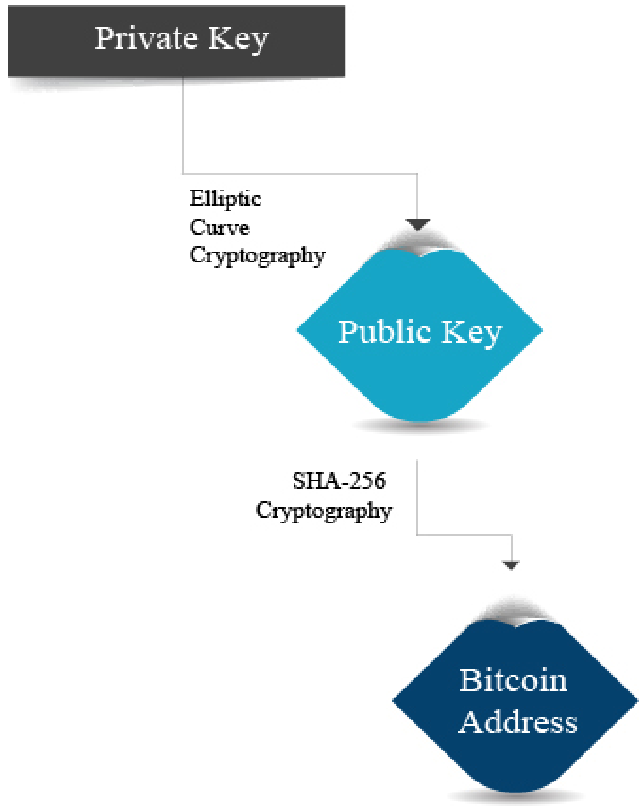
c. Step 3 – The Keys and the Bitcoin Address

Bitcoin uses a system of keys and cryptography — called public-key cryptography — to allow its users to trade safely without giving away any sensitive information.[63] The keys allow for "many of the interesting properties of bitcoin, including decentralized trust and control, ownership attestation, and the cryptographic-proof security model."[64] First, Alice and Bob will both need to create a *private key*, which is like a debit card pin number. Only the holder of the key should know this number and it is important to keep it backed up because if it is lost, it is gone forever. The private key will later be used to sign the transaction. Bitcoin wallet software will create a random private key number, made up of 256-bit binary numbers — meaning 256 random digits of zero or one.[65] This very long number can be compressed into a hexadecimal[66] format of 64 digits, where each digit represents 4 bits. For example: 1E99423A4ED276 08A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD.[67]

Using their private keys, Alice and Bob will each create a corresponding *public key*. The private to public key conversion is accomplished by using elliptic curve cryptography, which is mathematically different from SHA-256. For our purposes however, it is similar in that it is one-way cryptography so anyone with the public key will never be able to figure out the private key, but if you have the private key you will always get the same public key result.[68]

63. Brito et al., *supra* note 40, at 149.
64. ANTONOPOULOS, supra note 60.
65. *What Does 128-Bit Encryption Really Mean?*, CKWOP.ME.UK, http://www.ckwop.me.uk/What-does-128-bit-cryptography-really-mean.html (last visited May 24, 2015).
66. Hexadecimal format includes the first six letters of the alphabet and the numbers zero through nine.
67. ANTONOPOULOS, *supra* note 60.
68. For a thorough explanation of elliptic curve cryptography, see DARREL HANKERSON, GUIDE TO ELLIPTIC CURVE CRYPTOGRAPHY (2004).

Then, the public key will again go through a cryptographic transformation — this time using SHA-256 — to come up with the *Bitcoin address*. The Bitcoin address is a string of alphanumeric characters that signifies where Alice will send Bob's Bitcoin.[69] Bitcoin addresses start with the number "1", for example: 1J7mdg5rbQyUHENYdx39WVWK7fs LpEoXZy.[70] A Bitcoin address is similar to an invoice that a merchant sends out to its customers. Bob should create a new Bitcoin address for every transaction just like he would use a new invoice number for each customer. Bitcoin users can create as many keys and Bitcoin addresses as they wish. Alice will either need to know the exact address in which to send her Bitcoin, or more likely Bob will have a scannable QR code to which Alice may send the Bitcoin.[71]



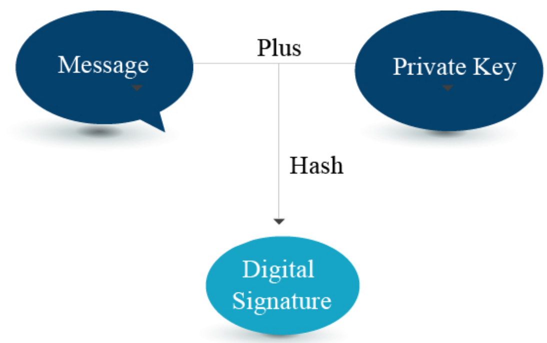
69. MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY 3 (2015).

70. Example taken from ANTONOPOULOS, *supra* note 60.

71. Timothy B. Lee, *12 Questions About Bitcoin You Were Too Embarrassed to Ask*, WASH. POST (Nov. 19, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/.

d. Step 4 – Signing the Transaction

Once Alice is ready with the message ("I want to send one Bitcoin to Bob" + last transaction hash) and Bob's Bitcoin address, Alice will sign this transaction using her *digital signature*. Just like the public key and Bitcoin address are derived from the private key, the digital signature is also cryptographically derived from the private key and the message. This is like signing a credit card receipt except that it is much more difficult to forge this signature. Note that any change in the message will alter the resulting digital signature, because the digital signature is derived from both the message and the private key.



e. Step 5 – Broadcast to the Network

Up to this point, everything can be done offline. Once all the correct parts are in place, Alice will need to connect to the Bitcoin network. Alice will then submit the request to transfer her Bitcoin to Bob and almost instantaneously everyone in the Bitcoin network can view this request including Bob's Bitcoin address and Alice's public key. This is where the *miners* come into play. Miners are essentially computers hooked up to the Bitcoin network that both serve to verify individual transaction, and to place those transactions within blocks on the Blockchain.

Miners will be able to determine the authenticity of Alice's signature just by knowing her public key number.[72] They do not need to know Alice's private key. They will take the message, digital signature, and Alice's public key number and this will create the transaction hash number for this particular transaction. Bob's new Bitcoin will remain encumbered until he is able to verify with his signature that he owns the Bitcoin address

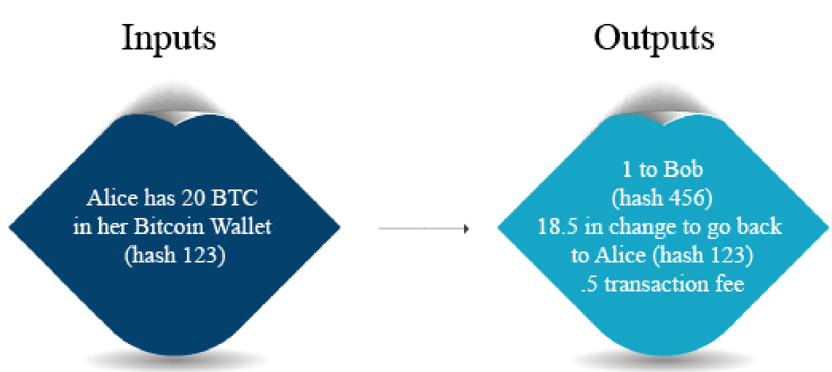
72. Brito et al., *supra* note 40, at 149.

that he told Alice to use.[73]

f. Step 6 – Transaction Fees

For simplicity in the above example, I left discussion of transaction fees out until now. A common misconception about Bitcoin is the idea that there are no transaction fees. In actuality, miners get a transaction fee on every transaction they successfully mine. There are two ways to earn transaction fees. First, anytime Alice wants to transfer Bitcoins to Bob, she must designate a portion of the transfer to go to the miners as a transaction fee. Second, any time a new block is successfully added to the Blockchain, brand new Bitcoins are released as a reward. For now, I will focus on the individual transaction fee.

Bitcoin transactions consist of inputs and outputs. The input consists of the previous transaction information — i.e., the amount and transaction hash from the Dad-Alice exchange. The output will always equal the same amount as the input,[74] just like it would on a balance sheet. The output will specify the amount to go to Bob, the amount that will need to remain with Alice in the form of change, and the transaction fee. Sometimes it takes several inputs to make one large output (e.g., if Mom, Dad, and Grandpa each gave Alice small amounts that equaled one Bitcoin), or Alice could use one input for several outputs (e.g., she wanted to pay Bob for pizza but Charlie for soda). Below is a modification of the above example where Alice's dad originally gave her twenty Bitcoins instead of one, and how this would break down as inputs and outputs:

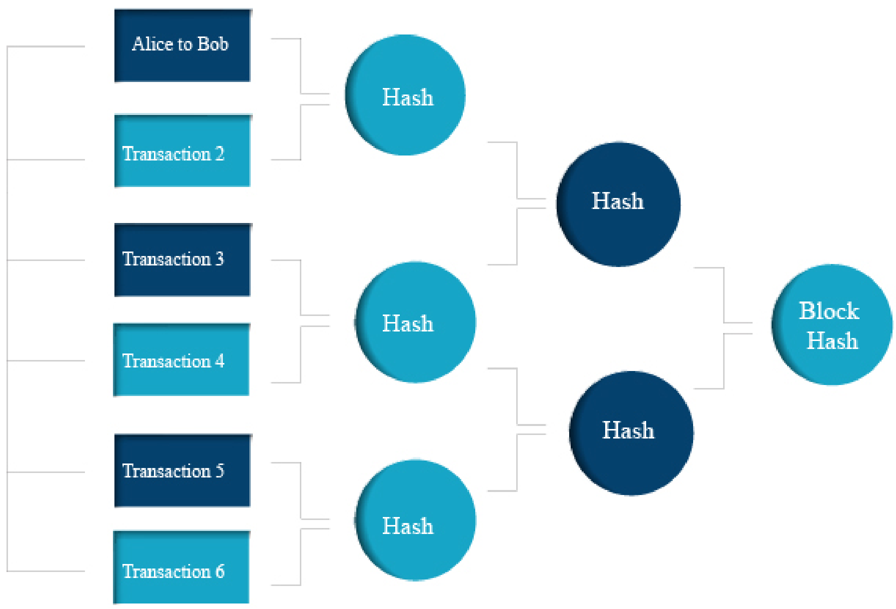


73. ANTONOPOULOS, *supra* note 60.
74. In actuality, the transaction fee is not listed explicitly in the Blockchain but is rather inferred, as the output will always be slightly less than the inputs.

2. Incorporating the Transaction into the Blockchain

Once the transaction has been verified, it will sit on the network unconfirmed until it is packed into several other transactions in a *block*. This process takes around ten minutes and this is the main aspect of the miners' job. The first step the miners will take is to collate all the recent transactions into a single transaction block. Think of a transaction like a proposed entry in a ledger and the block as a page out of the ledger.[75]

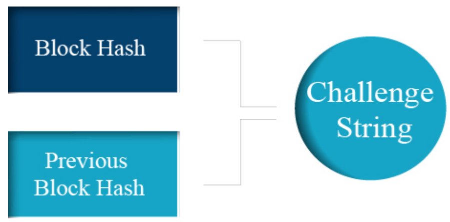
Once all of the recent transactions are organized into a proposed new block, the miners will go through a series of SHA-256 cryptographic hashes until all of the transactions result in one hash. To do this, miners will start with hashing all the transactions in pairs. The miners will then take those hashes and hash them in pairs, and will keep performing these iterations until finally there is just one final hash.



Then, miners will combine the block hash with the block hash from the previous block. Going all the way back to the *genesis block* — the very first block on the Blockchain — each block contains the block hash from the block before it. This is just like how each transaction contains a piece of the transaction before it in order to track Bitcoin transfers back to their

75. *Bitcoin: Transaction Block Chains*, KHAN ACADEMY, https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-transaction-block-chains.

individual inception. Miners will take the two block hashes and will run another SHA-256 hash to result in the hash that will be used in the proof-of-work formula (described further in the next section). This is called a *challenge string*. Miners will use this challenge string to help them solve a mathematical puzzle called proof-of-work and once this puzzle is solved the block will officially be added to the Blockchain.



3. Proving the Work

A Proof-of-Work system is sort of like a puzzle, requiring the miners to go through a lot of computational work in order to prove that a transaction is legitimate. Once the initial computational work is performed and the puzzle is solved, it is much easier to verify that the answer is the correct answer.

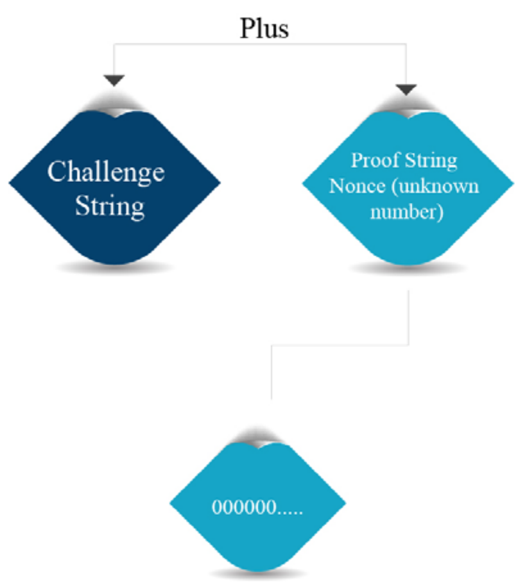
To break this concept down into something tangible,[76] imagine someone gave you the number 589 and then asked you to figure out the two prime numbers that make up 589. To figure it out, you would need to go through a lot of trial and error before finally discovering that 9 and 31 multiplied together equals 589. Once this initial work is performed, it is much easier for anyone else in the system to verify that this is correct by simply multiplying 9 and 31 together and seeing that 589 is correct.

Bitcoin's proof-of-work operates in this way but on a much more difficult level that requires very high computational effort. Bitcoin's puzzle is more like starting with a can of mixed paint and trying to figure out what colors and in what quantity went into the can. Of course, Bitcoin miners themselves are not trying to figure out these incredibly complex formulas with pen and paper or a calculator; their computers are doing these for them by making millions of guesses per second to try and solve the problem. This takes an immense amount of CPU and takes on average ten minutes to solve the puzzle.

76. This example comes from James Lyne, *Everyday Cybercrime — And What You Can Do About It*, TED (Feb. 2013), https://www.ted.com/talks/james_lyne_everyday_cybercrime_and_what_you_can_do_about_it?language=en.

First, miners will start with the challenge string (the final hash from the current block hashed with the previous block). Miners are going to search for the "proof" — that is the answer to the challenge. This proof string is also called a *nonce*. Miners know that when the challenge string and the correct proof string are taken together and hashed, the end result will be a number with certain mathematical properties — specifically the final result must contain a specified number of zeroes at its start.

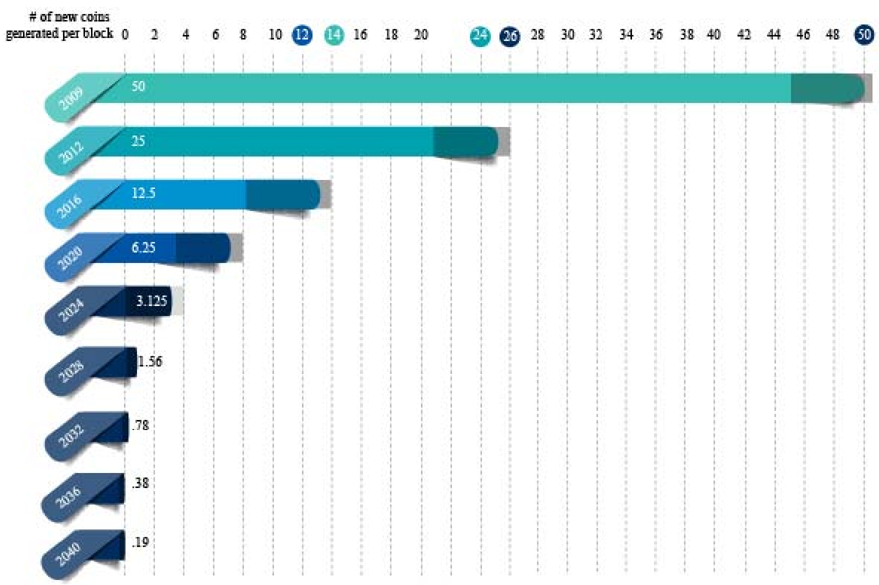
For example, in order to add the block containing Alice and Bob's transaction to the Blockchain, miners will be given a problem to solve and they will know the end result will start with 40 zeroes. In order to come up with a proof string that when combined with the challenge string and then hashed comes out to a number with 40 zeroes, miners will try a trillion different possibilities, and at some point one of the miners will come up with the correct answer. Once a miner discovers the correct proof string, he will broadcast the new block to all other active miners in the system.[77] The other miners will immediately shift from trying to solve the puzzle to verifying that all of the transactions are valid and that the proof string really solves the puzzle. The number of verifications a proof string receives acts as votes and the block with the most votes wins. The block will officially be added to the Blockchain and a new reward will be released. Miners will then begin working on the next block, using the hash of the previously accepted block.



77. Nakamoto, *supra* note 3, at 3.

a. Coinbase/Generation Reward

The reward released as a new block is added to the chain is called a *coinbase reward* (also called a generation reward). Just like mining for gold or any other precious metal, the more Bitcoin that is mined the more difficult it is to receive a reward. At Bitcoin's inception, a new block resulted in a 50 Bitcoin reward. Today, a new block results in a 25 Bitcoin reward. The coinbase reward will halve every few years until all 21 million Bitcoins are released, which is expected to happen in 2040. The chart below shows the number of new Bitcoins generated per block from 2009-2040.[78]



b. Difficulty Level

Nakamoto designed the level of difficulty in generating a new block to change every two weeks so that each transaction takes an average of ten minutes to process.[79] This is accomplished by changing the number of zeroes required at the beginning of the answer to the proof and challenge strings. The more zeroes, the more difficult the problem becomes to solve.

78. *Controlled Supply*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Controlled_supply (last visited Dec. 1, 2014).
79. *Protocol Rules*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Protocol_rules (last visited Dec. 1, 2014).

If it starts taking less than ten minutes, then the number of zeroes goes up, requiring more time to solve the problem. If it takes more than ten minutes, then the number of zeroes required will adjust downward. As more and more people are mining Bitcoin, the difficulty has increased exponentially in the past few years. Currently, it takes around forty billion attempts to come up with one correct proof string.[80]

c. Simultaneous Solving/Orphan Blocks

One last topic that is important to understand is the concept of simultaneous solving and orphan blocks. It is possible that two miners will solve for the proof string at the same time and create two identical blocks. This makes it confusing for the rest of the miners in trying to figure out which block to use for building on the next block. The tie is broken when the next proof is found, and one of the branches becomes longer than the other. In other words, the block with the most CPU associated with it will be the one that other miners accept as being the most accurate and verified block. Miners "express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash."[81] The rejected or *orphan blocks* will not last long as the rest of the system will stick with the accepted blocks.

C. Proof-of-Work Concerns and Alternative Systems

Although proof-of-work really revolutionized the way transactions are processed by allowing transactions to be handled peer-to-peer without a third party intermediary, it has some significant disadvantages. This section will address those disadvantages and then will highlight a few alternatives to proof-of-work.

1. Disadvantages of Proof-of-Work

The three most often cited disadvantages of proof-of-work are: (1) the computational effort required; (2) diminishing returns; and (3) a 51% attack. The alternative systems that will be discussed below mainly focus on fixing the first and most serious problem — the computational effort required. But first, each of these three issues will be discussed in turn.

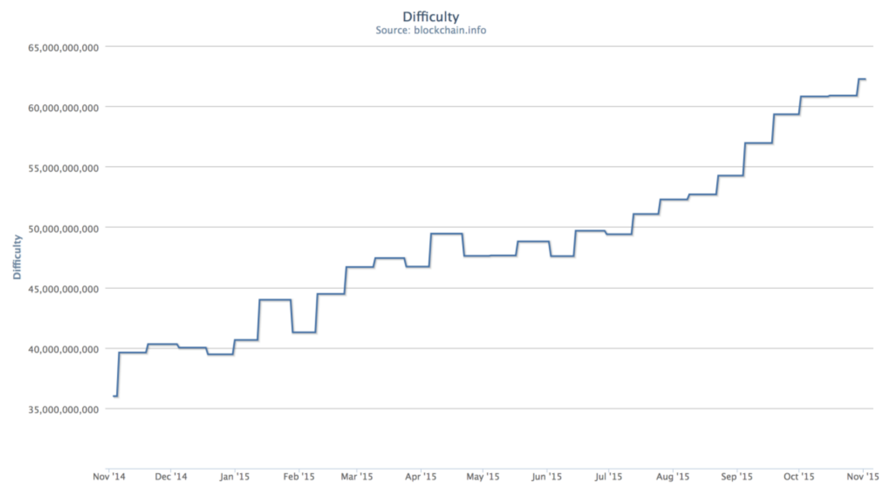
80. Anthony Volastro, *CNBC Explains: How to Mine Bitcoins on your Own*, CNBC (Jan. 23, 2014, 1:48 PM), http://www.cnbc.com/id/101332124.

81. Nakamoto, *supra* note 3, at 3.

a. Required Computational Effort (CPU)

Rather than giving each miner one vote and allowing majority vote to rule the day ("one-IP-address-one-vote"[82]), the Blockchain was designed with CPU in mind ("one-CPU-one-vote"[83]). Initially this seemed like a good idea because with majority vote "an attacker could game the system by creating numerous fake identities."[84] Proof-of-work is designed so that it is very costly to game the system.

However, the disadvantage of using CPU power as proof is the significant amount of energy that is required. Currently, performing these proof-of-work calculations burns through "173 megawatts of electricity continuously. For perspective, that amount is approximately 20 percent of an average nuclear power plant."[85] The energy required is estimated to cost around $600 million.[86] As mentioned above, as interest in Bitcoin has grown and more and more miners have joined the system, the difficulty level has adjusted upward and it results in a much higher level of energy expended. The chart below shows the difficulty level from November 2014-November 2015.[87]



82. Nakamoto, *supra* note 3, at 3.
83. *Id.*
84. Rainier Bohme et al., *Bitcoin: Economics, Technology, and Governance,* 29 J. OF ECON. PERSPECTIVES 213, 218–19 (2015).
85. *Id.* at 218.
86. William Mougayer, *The Blockchain is the New Database, Get Ready to Rewrite Everything*, STARTUP MGMT. (Dec. 27, 2014), http://startupmanagement.org/2014/12/27/the-blockchain-is-the-new-database-get-ready-to-rewrite-everything/.
87. *Difficulty*, BLOCKCHAIN INFO, https://blockchain.info/charts/difficulty (last visited Jan. 15, 2016).

b. Diminishing Returns

The concept of diminishing returns has many in the media concerned.[88] As more and more Bitcoins are mined, the coinbase reward will continue to get smaller until it disappears entirely. The argument is that once the reward disappears, miners will no longer be incentivized to mine, and because very few people will mine, the security of the entire system will be jeopardized. However, this concern may be overblown for two reasons. First, the fact is that most miners get their fees from the individual transactions and not from adding a new block to the chain, so it is unlikely that miners will be disincentivized to mine once all 21 million Bitcoins are released. Second, the Bitcoin system is designed with adjusting difficulty to take into account the changing number of miners and to ensure that mining is profitable.

c. 51% Attack

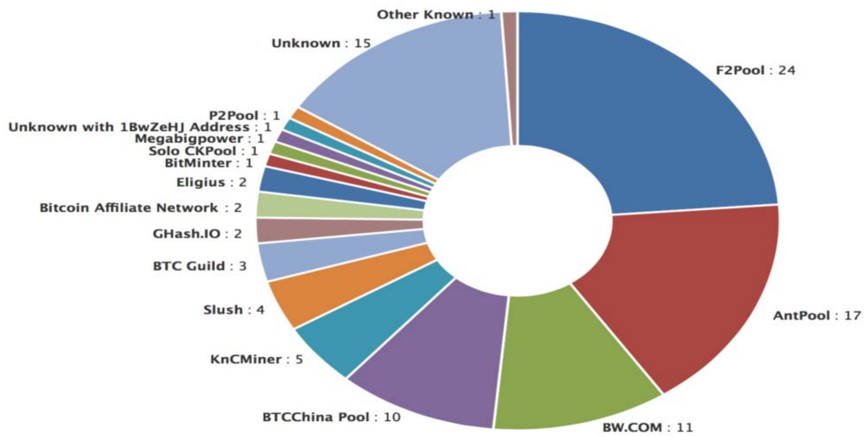
Although the Blockchain is incredibly secure, it is not immune from attack. Hacking typically occurs when someone breaks into an online exchange or online wallet provider and steals the Bitcoin keys stored on the site. Thus far, no one has ever broken into the actual Blockchain and stolen Bitcoins through that directly; it has always been through third-party Bitcoin storage providers.

In order for the actual Blockchain to be hacked, a miner or a pool of miners would have to attain 51% of the computing power, and then rewrite the Blockchain's history. At the beginning of Bitcoin's history, it was fairly easy to mine and required little computational power, and the potential for a 51% attack was a lot higher. However, "as time goes on and more powerful devices run legitimate copies of the software, it becomes extremely difficult for any single party to disrupt the system."[89] That said, as mining becomes more difficult, the demographics of miners have changed. "Individual home miners have given way to large operators that invest substantial money in mining farms in far away places with low

88. Maria Korolov, *Bitcoin Approaching Diminishing Returns*, HYPERGRID BUS. (Feb. 21, 2014), http://www.hypergridbusiness.com/2014/02/bitcoin-approaching-diminishing-returns/; Alec Liu, *A Guide to Bitcoin Mining: Why Someone Bought a $1,500 Bitcoin Miner on eBay for $20,600*, MOTHERBOARD (Mar. 22, 2013, 9:45 AM), http://motherboard.vice.com/blog/a-guide-to-bitcoin-mining-why-someone-bought-a-1500-bitcoin-miner-on-ebay-for-20600; Alec Liu, *How to Really Get Rich From Bitcoins*, MOTHERBOARD (Apr. 10, 2013, 9:40 AM), http://motherboard.vice.com/blog/how-to-really-get-rich-from-bitcoins.

89. Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. U. L. REV. Online 257, 262 (2014).

temperatures and low electricity costs."[90] Additionally, many miners have joined mining *pools* that allow them to collectively solve the proof-of-work and then split the reward between them. Below is a chart showing the percentages of Bitcoin mined by pools.[91]



These pools present a risk of centralization. This is not something Satoshi Hashimoto had in mind for Bitcoin,[92] but is becoming increasingly common. Last year some of the largest pools voluntarily split into smaller pools because the top two pools actually held a majority of the CPU power. The fear with centralization is that if one group holds a majority of the mining power (51%), then this group could effectively rewrite the entire Blockchain. As mentioned above, while it is theoretically possible that one group could hold the majority of mining power, even if it did it is not likely it would want to rewrite the Blockchain.[93] As soon as the majority CPU began rewriting the Blockchain, everyone else in the network would notice and the price of Bitcoin would plummet. Therefore, the fear of this threat appears to be overblown.

90. Giulio Prisco, *Mining Bitcoin is Big Business — the Economist*, CRYPTOCOINS NEWS (Jan. 10, 2015), https://www.cryptocoinsnews.com/mining-bitcoin-big-business-economist/.

91. *Hashrate Distribution*, BLOCKCHAIN INFO, https://blockchain.info/pools (last visited May 24, 2015). "Unknown" represents either individual miners, or more likely private or mining pools that require an invitation.

92. Nakamoto, *supra* note 3, at 1.

93. A while back a mining group was getting close to reaching a majority, and it voluntarily split into several small groups in order to ensure the integrity of the system. This is another reason why it is unlikely that a mining group would be able to throw the entire system. Robert McMillan, *Bitcoin Stares Down Impending Apocalypse (Again)*, WIRED (Jan. 10, 2014, 6:30 AM), http://www.wired.com /2014/01/ghash/.

2. Alternative to Proof-of-Work—Proof-of-Stake

Proof-of-stake is an alternative to using proof-of-work to verify digital transactions. Where proof-of-work weighs votes based on the amount of CPU devoted to the system, a proof-of-stake system weighs votes based on the number of Bitcoins a user owns.[94] Therefore, a person holding one percent of the total Bitcoins could mine one percent of the blocks.[95] This solves the problem of majority vote mentioned above (one-IP address-one-vote), because users must have a stake in the system before they can cast their votes. This is considered a better system because some are concerned that with the diminishing returns referred to in the previous section, the security of Bitcoin transactions will decrease over time. If instead the votes are based on the miner's ownership, the miner is incentivized to ensure the transactions are accurate because it has a "stake" in the future performance of the currency.

Where the fear with proof-of-work is diminishing returns, the fear with proof-of-stake is monopoly problems. In proof-of-stake, if a user gains 51% of the outstanding coins, then it:

> could use these resources to impose conditions on the rest of the network. Potentially, the monopolist could choose to do this in malicious ways, such as double spending or denying services. If the monopolist chose a malicious strategy and maintained his control for a long period, confidence in bitcoin would be undermined and bitcoin purchasing power would collapse.[96]

However, just like with proof-of-work, anyone reaching a majority of the control of the number of Bitcoins would be unlikely to undermine the system because then Bitcoin would lose its value and potentially billions of dollars. Other users will quickly notice that the fifty-one percenter is up to no good and then "the public will lose faith in Bitcoin, and the value of Bitcoins will plummet. So the act of stealing will render the fruits of the theft worthless."[97] Following is a chart showing a summary of proof-of-work versus proof-of-stake:

94. This idea is thought to have originated on a bitcointalk thread in 2011 by member QuantumMechanic. QuantumMechanic, *Proof-of-stake Instead of Proof-of-work*, BITCOIN TALK (July 11, 2011, 4:12 AM), https://bitcointalk.org/index.php?topic=27787.0.

95. *Proof-of-stake*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Proof_of_Stake (last visited Dec. 1, 2014).

96. *Id.*

97. Ed Felten, *Bitcoin Mining Now Dominated by One Pool*, FREEDOM TO TINKER (June 16, 2014), https://freedom-to-tinker.com/blog/felten/bitcoin-mining-now-dominated-by-one-pool/.

	Proof-of-work	Proof-of-stake
How Voting Works	Computational power (CPU)	Stake in the currency
Advantages	• Ensures accuracy/validity of transactions • Not required to own a lot of Bitcoin – removes incentive to hoard	• low CPU required • allows those with the most "stake" or skin in the game the highest votes
Disadvantages	• Uses a lot of power – bad for the environment • Diminishing returns • Potential for 51% attack	• Potential for monopolization • Encourages hoarding

a. An Example of Proof-of-Stake—NXT

To date, the most successful Bitcoin alternative (*altcoin*) using a pure proof-of-stake system is *NXT*. Instead of miners, the system uses "forgers" who forge the transactions into blocks.[98] Forgers are selected to forge a particular block at random with the odds of selection being proportional to the forgers' stake in the network — i.e., the number of NXT coins they hold.[99] A new block can be added to the chain approximately every sixty seconds, instead of ten minutes.[100] One unique feature of NXT is that it allows users to forge on their cell phone or home computer — there is no need for fancy mining hardware like that required by Bitcoin. Another interesting feature is that forgers do not get a reward for each new block in the system, they only get transaction fees from the individual transactions.

NXT also solved the potential 51% attack problem by implementing "transparent forging," which is defined as the following:

> Although the [forger] which forges a block is random in the long term, in the immediate future it is highly predictable. This means the network knows where the next block should be forged. If a [forger] does not forge the block it is

98. *Whitepaper: NXT*, NXT WIKI, http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt#Block_Creation_.28Forging.29 (last visited Apr. 8, 2016).
99. *Id.*
100. *Id.*

> expected to (perhaps because it is working to build a fraudulent chain instead), it is excluded from the network for a period of time. The likelihood of that [forger] being chosen is instead redistributed across the remaining members of the network.[101]

NXT is also designed not just for cryptocurrency, but also to include asset transfers, an online marketplace, private messaging, and the option to create your own currency that is backed by NXT.[102] In the future, NXT plans on adding voting capabilities, smart contracts, and instant transactions.[103]

b. A Twist on Proof-of-Stake — Delegated Proof-of-Stake

The company Bitshares uses delegated proof-of-stake to secure its Blockchain. Delegated proof-of-stake requires 51% of the stakeholders to agree on the new transactions before they can be added to the Blockchain. However, to save time and increase efficiency, the system allows stakeholders to "delegate their voting power to a delegate. The top 100 delegates by total votes take turns generating blocks on a defined schedule."[104] In order to become a delegate, a user must post a small bond. When a delegate behaves badly, i.e., signing in invalid block, failing to produce a block, or failing to reference the previous block, the system will "automatically vote against that delegate the next time their user makes a transaction until that delegate is no longer" able to perform the role of delegate.[105]

3. Mixed Proof-of-Work/Proof-of-Stake

Most of the other altcoins that do not rely exclusively on proof-of-work use some sort of combination of proof-of-work plus proof-of-stake or something else entirely. In August 2012, *Peercoin* was the first altcoin "to use a hybrid proof-of-work and proof-of-stake algorithm to issue new currency."[106] Peercoin uses proof-of-stake to keep the Blockchain secure

101. *What Is Transparent Forging?*, ABOUT NXT, http://nxt.org/about/proof-of-stake/ (last visited May 24, 2015).

102. *Id.*

103. *Upcoming Features*, ABOUT NXT, http://nxt.org/about/proof-of-stake/ (last visited May 24, 2015).

104. Daniel Larimer, *Delegated Proof-of-stake*, BITSHARES (Apr. 3, 2014), http://bitshares.org/blog/delegated-proof-of-stake/.

105. *Id.*

106. Antonopoulos, *supra* note 60.

and uses proof-of-work to enable the reward associated with completing a new block.[107] Like Bitcoin, the difficulty level is adjusted so that there is ten minutes between transactions, however with Peercoin this difficulty level adjusts after every block is completed and not once every two weeks. This allows for the difficulty level to more accurately reflect reality and keep the transaction time as close as possible to ten minutes.

The company NEM uses "proof-of-importance" to reward the users who "actively participate in the economy. The balance of an account, who transacts with them, and how much they transact to others are all combined to calculate an account's importance."[108] Instead of miners or forgers, NEM uses harvesters to do the work of verifying transactions.[109] Harvesters must have a stake or vested balance of at least 10,000 of NEM's currency (called "XEM").[110] New blocks are harvested once every minute in NEM's system.[111]

4. Other Innovations

The Blockchain is already being used for a variety of purposes outside of just cryptocurrency transfers. Currency exchange and remittances, smart contracts, smart property, charitable proof-of-work, and domain name registration are just a few of the innovations currently available.

a. Currency Exchange and Remittances — Ripple

Ripple has the second-highest market capitalization next to Bitcoin at $220 million.[112] Ripple created a cryptocurrency called ripples, but also acts as a currency exchange and remittance network. Ripple supports fiat currency (U.S. dollars, euros, etc.), other cryptocurrencies (Bitcoin, Litecoin, etc.), commodities, and even frequent flier miles. Ripple uses a Blockchain called the "Ripple ledger" that keeps track of all the transactions in the system.

Ripple also uses "gateways" to enable transfers from one form to another. Gateways are other people or companies that use the Ripple network to make exchanges. Typically, one gateway will convert the asset

107. Sunny King & Scott Nadal, *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, PEERCOIN (Aug. 19, 2012), http://peercoin.net/assets/paper/peercoin-paper.pdf.

108. Alireza Beikverdi, *NEM Launches, Targets Old Economy with Proof-of-Importance*, COINTELEGRAPH (Apr. 1, 2015, 8:14 AM), http://cointelegraph.com/news/nem-launches-targets-old-economy-with-proof-of-importance.

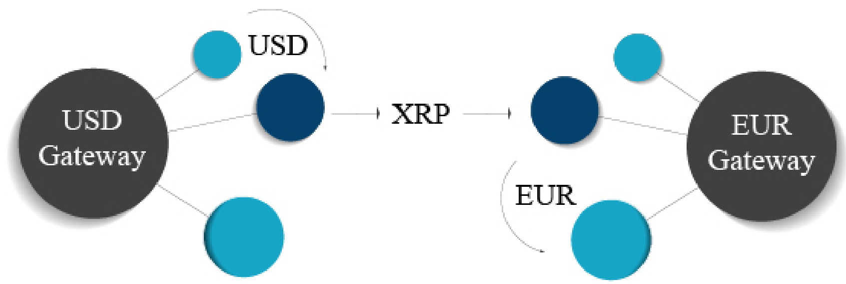
109. *FAQs*, NEM, http://www.nem.io/faq.html (last visited May 24, 2015).

110. *Id.*

111. *Id.*

112. *Crypto-Currency*, *supra* note 1.

into ripples which will act as a vehicle currency to enable the exchange into another asset. For example, if Alice has $200 and she wants to trade it for euros, she will send her money to one gateway that will convert her money into ripples and then will send the money to another gateway that will trade the ripples for euros and then send it back to her.



This illustration provides a visual example of exchanging U.S. dollars into euros, using ripples as the transaction vehicle.[113]

The biggest advantage of Ripple is probably for expatriates wishing to send money back to their home countries. Depending on the country and currency, it can take several days and cost a lot of money to make these remittances.[114] Transaction fees can eat up to twelve percent of these hard-earned payments.[115] Transaction fees on Ripple comes out to around 1/100th of a penny.[116] Also, Ripple is incredibly fast compared to traditional remittance services and even fast compared to Bitcoin. It takes anywhere from two to twenty seconds to confirm a transaction.[117]

Ripple uses a consensus algorithm to approve new transactions that is similar to delegated proof-of-stake. Ripple miners work in small groups to approve transactions, and eighty percent of the group must approve before the transaction is approved.[118] This means that 80% of the network — as opposed to 51% — would have to be acting maliciously before someone could upset the network. Ripple also employs proof-of-work in order for the miners to join the small groups.[119] The existing miners will generate a

113. *Ripple for Market Makers*, RIPPLE, https://ripple.com/trade/ripple-for-market-makers/ (last visited May 24, 2015).

114. Tom Simonite, *Making Money: Ripple Labs*, MIT TECH. REV. (Feb. 18, 2014), http://www.technologyreview.com/featuredstory/524566/making-money/.

115. *Id.*

116. 1/1000 vs 1/100; Ariella Brown, *10 Things You Need to Know About Ripple*, COINDESK (May 17, 2013, 11:00 AM), http://www.coindesk.com/10-things-you-need-to-know-about-ripple/.

117. *Ripple*, *Supra* note 113.

118. David Schwartz et al., *The Ripple Protocol Consensus Algorithm*, RIPPLE LABS (2014), https://ripple.com/files/ripple_consensus_whitepaper.pdf.

119. *Proof-of-work*, RIPPLE, https://wiki.ripple.com/Proof_of_Work (last visited May 24, 2015).

challenge string that the new miner will need to answer before he or she can join the group. This makes the cost of attacking the system prohibitively expensive.[120]

b. Smart Contracts — Ethereum

In 1997, Nick Szabo first introduced the concept of smart contracts in his paper "The Idea of Smart Contracts."[121] Smart Contracts are "automated programs that transfer digital assets within the blockchain upon certain triggering conditions."[122] Like the Blockchain itself, smart contracts "subsist independently of any moral or legal entity."[123] Instead, two parties use coding to create:

> a little program that you can entrust with a unit of value (as a token or money), and rules around that value. The basic idea behind smart contracts is that a transaction's contractual governance between two or more parties can be verified programmatically via the blockchain, instead of via a central arbitrator, rule maker or gatekeeper . . . . [The parties] can bake the terms and implications of their agreement programmatically and conditionally, with automatic money releases when fulfilling services in a sequential manner, or incur penalties if not fulfilled.[124]

The Blockchain replaces the role of the third party typically required to resolve disagreements. As an example,

> imagine a red-widget factory receives an order from a new customer to produce 100 of a new type of blue widget. This requires the factory to invest in a new machine and they will only recoup this investment if the customer follows through

120. *Proof-of-work*, *supra* note 119.

121. Nick Szabo, *The Idea of Smart Contracts*, NICK SZABO'S PAPERS AND CONCISE TUTORIALS (1997), http://szabo.best.vwh.net/idea.html.

122. Joshua A.T. Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 36, 38 (2014).

123. Primavera de Filippi, *Tomorrow's Apps Will Come from Brilliant (and Risky) Bitcoin Code*, WIRED (Mar. 8, 2014, 6:30 AM), http://www.wired.com/2014/03/decentralized-applications-built-bitcoin-great-except-whos-responsible-outcomes/.

124. William Mougayar, *The Blockchain is the New Database, Get Ready to Rewrite Everything*, STARTUP MGMT. (Dec. 27, 2014), http://startupmanagement.org/2014/12/27/the-blockchain-is-the-new-database-get-ready-to-rewrite-everything/. *See also* Melanie Swan, *Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization)*, MS FUTURES GROUP (Apr. 2, 2015), http://www.melanieswan.com/documents/BlockchainThinking_SWAN.pdf.

> on their order. Instead of trusting the customer or hiring an expensive lawyer, the company could create a smart property with a self-executing contract. Such a contract might look like this: For every blue widget delivered, transfer price per item from the customer's bank account to the factory's bank account. Not only does this eliminate the need for a deposit or escrow — which places trust in a third party — the customer is protected from the factory under-delivering.[125]

Smart contracts could be used for virtually anything that can be owned—tangible property like homes, cars, phones, and computers, and intangible property such as intellectual property rights could all be purchased using smart contracts.[126] This could easily be implemented with car purchases. A car could contain code that is tied to the smart contract.[127] If the borrower becomes late on a car payment, the parties could agree on a code that would forbid the keys from opening the car until the default is cured. If it gets to the point where the lender needs to repossess the car, the code could automatically provide that the lenders keys could open the door in that situation. Finally, when the final payment is made, the smart contract could provide that the lender no longer has any legal rights to the car, and the borrower has full rights.

Ethereum is the most highly anticipated platform for smart contracts. Rather than building off of the Bitcoin network, Ethereum created its own Blockchain from scratch.[128] It uses some of the proof-of-work and proof-of-stake aspects of other Bitcoins, but also includes a built-in Turing-complete programming language.[129] This means that instead of creating a different platform for each individual application, Ethereum developed one programming language that is powerful enough to build any other program or application of top of the underlying language.[130] This is like how Gmail, Facebook, and countless other applications are built on top of JavaScript. Ethereum supports several programming languages, including C++ and

125. Josh Blatchford, *4 Ways Blockchain Technology will Change the World*, VENTUREBEAT (Mar. 28, 2015, 7:00 AM), http://venturebeat.com/2015/03/28/4-ways-blockchain-technology-will-change-the-world/.

126. *Smart Property*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Smart_Property (last visited Dec. 1, 2014).

127. Nick Szabo originally gave an example like this in his 1997 paper. Szabo, *supra* note 120.

128. Ethereum, *Vitalik Buterin Reveals Ethereum at Bitcoin Miami 2014*, YOUTUBE (Feb. 1, 2014), https://www.youtube.com/watch?v=l9dpjN3Mwps.

129. Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, GITHUB, https://github.com/ethereum/wiki/wiki/White-Paper#blockchain-and-mining (last updated Apr. 29, 2015).

130. Ethereum, *supra* note 128.

JavaScript.[131]

Ethereum also uses a stack-based language in order to create a virtually unlimited number of stages in the contract. With Bitcoin, the transactions are binary — the Bitcoin are either spent or not spent. With Ethereum, the contract does not have to be fulfilled or unfulfilled, but can be in stage one pre-negotiation, stage two offer, etc.

Ethereum also created its own cryptocurrency called *ether*. Ether is used as a token to represent the asset virtually. Users can create their own currencies on top of ether just like NXT. Ethereum plans to release 15 million ethers each year, and, unlike Bitcoin, there is no cap.[132] Ethers are required in order to create contracts or even to run Ethereum's software, and is referred to by Ethereum's founders as the "platform's programming 'fuel.'"[133]

c. Colored Coins

Colored coins takes Bitcoin and adds on a piece of code in order to represent an asset — like smart property. In effect, it changes the color of the coin so that you know the type of asset, where the asset has been, and where it is going. For example, you could use colored coins technology to add code to a Bitcoin specifying that the Bitcoin represents your house, changing the Bitcoin into effectively a token to represent the value of your house. This could be done with securities, cars, or any other type of property. Ethereum used the concept of colored coins as a facet of its platform, only with Ethereum the colored coins are not tied to Bitcoin but rather ether.

d. Charitable Proof-of-work

Several alternative cryptocurrencies have been proposed or are now in motion that use the proof-of-work process to perform something useful for society, meaning they solve problems using their algorithms. One such example is CureCoin, who partnered up with Stanford University's Folding@home program.[134] The Folding@home program seeks to use the power of the cloud to study and find cures for cancer, Alzheimer's,

131. Robert McMillan, *Project to Turn Bitcoin into an All-Powerful Programming Language Raises $15M*, WIRED (Sept. 10, 2014, 6:30 AM), http://www.wired.com/2014/09/ethereum-backers-raise-15-million/.
132. *Id.*
133. *Id.*
134. *What Is CureCoin?*, CURECOIN, https://www.curecoin.net/index.php/knowledge-base/14-knowledge-base/about-curecoin/19-what-is-curecoin (last visited May 24, 2015).

Parkinson's, and many other diseases.[135] Instead of Bitcoin miners solving some arbitrary puzzle, CureCoin miners use their CPU to fold proteins and receive CureCoin rewards based on the amount of CPU contributed. Another proof-of-charity company is Primecoin, who uses proof-of-work to discover new prime numbers.[136]

e. Namecoin

Namecoin was the first Bitcoin fork — meaning the first company to take the Bitcoin Blockchain and create its own Blockchain using the exact same technology.[137] As such, Namecoin is very similar to Bitcoin with a ten minute transaction time, 21 million cap on the total number of Namecoin, and the same rewards released with each new block. One major difference is that with Namecoin users can store information in addition to just the transaction information on the Blockchain. Specifically, Namecoin is a decentralized Domain Name System ("DNS"). The DNS allows internet users to type in a URL address rather than requiring a specific IP address. For example, entering "'google.com' into your browser will trigger your computer to check its DNS server for Google's IP address."[138] The benefit of a decentralized DNS is that it cannot be censored or shut down, just like Bitcoin.

D. PLATFORM RECOMMENDATIONS FOR A CRYPTOSECURITIES MARKET

A cryptosecurities market would require certain unique features. First, unlike Bitcoin, shares cannot be divided into small units but can trade only in whole numbers. Second, Bitcoin miners are paid transaction fees in Bitcoin, but in a cryptosecurities market you cannot pay the miners with shares. Third, the securities will need to have technology that enables issuers to specify the type of security, whether stock, bond, etc.

The technology already exists to create a cryptosecurities market. Using a platform such as Ripple or Ethereum, a cryptosecurities system could easily be built onto the existing code. Then, the colored coin technology could specify the type of security offered, and any restrictions on the securities. Ethereum has the capability of processing transactions in less than a minute, and Ripple confirmations take only a few seconds.

135. START FOLDING, https://folding.stanford.edu (last visited May 24, 2015).
136. *Id.*
137. NAMECOIN, https://namecoin.info (last visited May 24, 2015).
138. David Gilson, *What Are Namecoins and .bit Domains?*, COINDESK (June 18, 2013, 1:30 PM), http://www.coindesk.com/what-are-namecoins-and-bit-domains/.

IV. PROBLEMS WITH THE STOCK MARKET AND HOW A CRYPTOSECURITIES MARKET WOULD ADDRESS THESE ISSUES

Many argue that the stock market is broken.[139] Occupy Wall Street, *The Wolf of Wall Street*, and high-frequency trading are all notorious examples illuminating why there is a problem, and why now is the time to address these problems. This section highlights some issues with the current stock market, and how a cryptosecurities market would address and solve these problems. Just as cryptocurrencies are an alternative to traditional currencies for those wishing to use them, the cryptosecurities stock market would be an alternative to the current stock market and not a replacement. Investors may choose to use this market in addition to or instead of traditional stock using traditional exchanges or brokerages.

A. PROBLEMS WITH STOCKBROKERS

There is likely not a better embodiment of all that is wrong with stockbrokers than that of Jordan Belfort — the self-proclaimed "Wolf of Wall Street." Belfort scammed investors out of more than $100 million dollars before being convicted and sentenced to federal prison. His over-the-counter brokerage firm, Stratton Oakmont, participated in several "pump and dump" schemes, wherein the company would purchase cheap stock, issue false and misleading statements in order to pump up the price of that stock, and then sell or dump the stock at the artificially inflated price. A reporter likened Belfort to a "twisted Robin Hood who takes from the rich and gives to himself and his merry band of brokers."[140]

While Mr. Belfort's actions stand out as particularly culpable, stockbrokers and dealers often engage in various activities that range from outright fraudulent to slightly less than legal. Although a large amount of trading today happens online, these trades must still go through an online brokerage, and that brokerage gets to decide how the trade will be executed (whether it will go through an exchange, market maker, etc.[141]) and gets to collect a commission on every trade.

139. After the publication of "Flash Boys" — the latest book by author Michael Lewis — SEC Chair Mary Jo White defended the stock market by claiming that it is not rigged and that the "U.S. markets are the strongest and most reliable in the world." Peter Hamner, *Wall Street and SEC Chief Respond to 'Flash Boys' Book*, KNOWLEDGE EFFECT (May 8, 2014), http://blog.thomsonreuters.com /index.php/ wall-street-and-sec-chief-respond-to-flash-boys-book/.

140. Brian Solomon, *Meet the Real 'Wolf of Wall Street' in Forbes' Original Takedown of Jordan Belfort*, FORBES (Dec. 28, 2013, 12:24 PM), http://www.forbes.com/sites/briansolomon/2013/12/28/ meet-the-real-wolf-of-wall-street-in-forbes-original-takedown-of-jordan-belfort/.

141. *Trade Execution: What Every Investor Should Know*, SEC, http://www.sec.gov/investor/pubs/ tradexec.htm (last updated Jan. 16, 2013).

If an investor prefers an actively managed mutual fund, then the brokers get an even bigger cut. Numerous studies have shown that actively managed mutual funds generate a lower return for investors than mutual funds sold to the investors directly.[142] It is illegal to switch a customer from one mutual fund into another when the new investment will not result in any net gain to the customer. But brokers do this all the time to generate commissions, and this is called "churning."

A cryptosecurities market would solve the broker problem simply by eliminating the mandatory requirement of going through a broker. Of course, less savvy or less involved investors could still choose to go through brokers, exchanges, actively managed funds, and other investment trusts, but others could make trades completely on their own or peer-to-peer, just like many Bitcoin users today.

B. HIGH FREQUENCY TRADING

Just as trading floors replaced outdoor curbside stock markets, high frequency trading ("HFT") has replaced trading floors by allowing computers to replace the work of human traders. HFT has allowed an exponential growth in the number of quotes. In 1999, around 1,000 quotes were received per second. By 2013, with the help of HFT computers, around 2,000,000 quotes go through every second even though there is less trading overall.[143] High-frequency trading firms make up around fifty percent of all stock trades.[144]

Proponents of HFT argue that it lowers costs, tightens spreads, and adds liquidity to the markets.[145] The bid-ask spread is "the difference in price between the highest price that a buyer is willing to pay for an asset and the lowest price for which a seller is willing to sell it."[146] The bid-ask spread has decreased over the past thirty years from about .20% to around .0002%, and some claim this is due to high-frequency trading and the

142. *See, e.g.*, Diane Del Guercio & Jonathan Reuter, *Mutual Fund Performance and the Incentive to Generate Alpha*, 69 J. OF FIN. 1673 (2014).

143. Richard Finger, *High Frequency Trading: Is it a Dark Force Against Ordinary Human Traders and Investors?*, FORBES (Sept. 30, 2013, 8:41 AM), http://www.forbes.com/sites/richardfinger/2013/09/30/high-frequency-trading-is-it-a-dark-force-against-ordinary-human-traders-and-investors/.

144. Peter J. Henning, *'Spoofing,' a New Crime With a Catchy Name*, N.Y. TIMES (Oct. 6, 2014, 12:39 PM), http://dealbook.nytimes.com/2014/10/06/a-new-crime-with-a-catchy-name-spoofing/.

145. Bruno J. Navarro, *High-Frequency Trading Benefits Investors: Advocate*, CNBC (Apr. 2, 2014, 2:46 PM), http://www.cnbc.com/id/101549113#.

146. *Bid-Ask Spread*, INVESTOPEDIA, http://www.investopedia.com/terms/b/bid-askspread.asp (last visited May 25, 2015).

resulting increased liquidity.[147]

But critics of HFT argue that HFT firms are getting all the reward without taking any of the risk. Traditionally, market makers were obligated to keep the markets in order and would "step in and be the buyer of last resort."[148] HFT firms are not taking on that kind of risk and have even bragged about not having a single day of trading losses over the course of several years.[149] Stephen Weiss of Short Hills Capital argued that HFT firms are ". . . not adding liquidity. They're sucking it out and returning it at a higher price after they've scalped you."[150]

Some major issues with HFT could be solved by using cryptosecurities. First, experiences like the flash crash would be avoided because it takes time to verify the transactions — even the fastest crypto-technologies require several seconds before transactions are completed. Second, spoofing and naked short selling would be impossible because you must actually hold the cryptostock before you could make a trade. If a trader does not have the stock in his crypto-portfolio, he will not be able to create the private and public keys necessary to make the trade.

1. The Flash Crash

On May 6, 2010, something unprecedented happened to the stock market. In only twenty minutes, investors lost around $862 billion.[151] Throughout history, the market has experienced crashes, but this was the largest single day point drop for the Dow Jones Industrial Average.[152] What makes this day truly unique among all other market crashes, however, is that within fifteen minutes, the market had bounced back up to almost exactly where it started that day.[153]

Over the same fifteen minutes, individual stocks traded wildly, with huge and evidently illogical price swings. Proctor & Gamble — a blue-

147. .0002 vs .002; Tim Worstall, *HFT Really Does Reduce the Bid Ask Spread; Making Michael Lewis Wrong About HFT*, FORBES (Apr. 1, 2014, 12:16 PM), http://www.forbes.com/sites/timworstall/2014/04/01/hft-really-does-reduce-the-bid-ask-spread-making-michael-lewis-wrong-about-hft/.

148. Finger, *supra* note 143.

149. MICHAEL LEWIS, FLASH BOYS: A WALL STREET REVOLT 109 (2015). "Virtu Financial publicly boasted that in five and a half years of trading it had experienced just one day when it hadn't made money, and that the loss was caused by 'human error.' In 2008, Dave Cummings, the CEO of a high-frequency trading firm called Tradebot, told university students that his firm had gone four years without a single day of trading losses. This sort of performance is possible only if you have a huge informational advantage." *Id.*

150. Henning, *supra* note 144.

151. Edgar Ortega Barrales, *Lessons from the Flash Crash for the Regulation of High-Frequency Traders*, 17 FORDHAM J. CORP. & FIN. L. 1195, 1196 (2012).

152. *Id.* at 1196–97.

153. Charles R. Korsmo, *High-Frequency Trading: A Regulatory Strategy*, 48 U. RICH. L. REV. 523, 525–26 (2014).

chip component of the benchmark Dow Jones Industrial Average ("DJIA") — dropped by 63% in less than four minutes, and then fully recovered in less than a minute. 3M experienced a similarly rapid collapse and recovery. Accenture, a multi-billion-dollar consultancy firm, saw its stock price fall from forty dollars per share to a penny in a matter of seconds, and then rocket back to forty dollars just as quickly. Shares of Apple, which had been trading at around $250 per share, changed hands at the outlandish price of $100,000 per share. Hundreds of other securities experienced similar chaos.[154]

Because it takes an average of ten minutes for a new block to be added to the Blockchain, it allows enough time to verify each transaction before it is added to the ledger as a verified transaction for everyone to see. Likewise, a cryptosecurities market would require several minutes for a transaction to process, which would help smooth out the issues caused by computer algorithms responding to imaginary signals that the market is starting to drop.

Of course, the SEC could create new rules requiring transactions to be verified and slowed down before being added to the system. However, this would not solve the other issues: brokers would still be required and traders could not trade peer-to-peer without third parties, and the trades could not be completed anonymously. Finally, a cryptosecurities market would not need to replace the stock market; it is merely an alternative that investors may use in addition to what is already out there.

2. Spoofing and Naked Short Selling

Another issue gaining attention with high frequency trading is "spoofing" or "layering." Spoofing occurs when a "trader places orders with no intention of having them executed but rather to trick others into buying or selling a stock at an artificial price driven by the orders that the trader later cancels."[155] The Dodd-Frank Act specifically lists spoofing as one of its prohibited transactions.[156]

A similar issue occurs with naked short selling. First, a short sale occurs when a trader borrows shares and then sells those shares without actually owning them. Say ABC stock is selling at $100 per share.[157] Bob wants to buy fifty shares. Alice borrows fifty shares from a brokerage and

154. Korsmo, *supra* note 153.

155. Press Release, SEC, SEC Charges N.Y.-Based Brokerage Firm with Layering (Sept. 25, 2012), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171484972#.VD1Vf77XFG4.

156. Dodd-Frank Act, 7 U.S.C. § 6c(a)(5)(C) (2012).

157. This example is loosely based on one found in this article: James J. Angel & Douglas M. McCabe, *Business Ethics of Short Selling and Naked Short Selling*, 85 J. BUS. ETHICS 239, 240 (2009).

sells them to Bob at $100 per share. The brokerage will deliver the shares to Bob and after three days the transaction is finalized.[158] When it comes time to pay for the borrowed shares, ABC stock has dropped to $80 per share. Alice therefore made a profit of twenty dollars per share minus fees charged by the brokerage. Conversely, if ABC stock rises after Bob buys the shares at $100 to $120, then Alice would lose $20 per share.

Naked short selling occurs when a seller has no intention of delivering the purchased shares on the settlement date (usually the third business day after the trade), or possibly has no intention of delivering the shares *at all*. The latter typically occurs when a trader is purposely trying to drive the stock price downwards to an artificially low stock price, which in turn "may cause serious damage to the firm by damaging its reputation as a going concern or by preventing the firm from obtaining needed financing."[159] The trader will not even borrow the shares before the "sale" takes place because the trader has no intention of completing the transaction. Settlement failures, whether purposeful or accidental, account for approximately 20% of total trades.[160]

A cryptosecurities market would cure any issues with spoofing and naked short selling because the system is not updated with the trade until the trade is complete. If a person places an order and then withdraws before the order is completely, it simply never shows up on the Blockchain ledger. This should increase the overall stability of the market and the stock value of the participating companies.

C. Other Advantages of a Cryptosecurities Market

The other main advantages of a cryptosecurities market are transparency, the fast settlement periods, the ability to trade twenty-four hours per day, and cheaper transaction costs.

1. Transparency

All transactions on the Blockchain are public and can be traced from origin through to present day. There are two types of traders that will appreciate this transparency. First are the traders dissatisfied with the status quo and dark pool trading, who feel that the system is corrupt because of all the secret trading and problems on Wall Street. The second

158. Once trades are completed, the trades are not settled until the third business day after the trade has processed, meaning the buyer does not actually pay for the shares or receive the stock certificate until the settlement date. Angel, *supra* note 157.
159. *Id.* at 242.
160. *Id.*

group of traders are those technologically savvy traders who enjoy the new technological aspect of trading on a cryptosecurities market. Therefore, the traders will include the two groups from the broad ends of the spectrum.

2. *Improved Speed*

Although high frequency traders can make trades in microseconds, the actual transfer of stocks takes up to three days.[161] This is how spoofing and naked short selling is able to occur. Because cryptosecurities trade on the Blockchain and are verified in less than one minute, this makes ownership rights clear and removes the opportunity for traders to take advantage of the system by spoofing or naked short selling. Additionally, the Blockchain runs twenty-four hours per day so traders would never have to worry about after-hours trading.

3. *Cheaper Transaction Costs*

There is a potential to significantly cut down on transaction costs with this a cryptosecurities market. With removing the requirement of brokers, and removing the need for transfer agents, the only fees left will be to the crypto-exchanges (unless the traders trade directly peer-to-peer) and to the SEC. The SEC charges exchanges fees that are kept "as close as possible to the amount of the regular appropriation to the Commission by Congress for that fiscal year. If transaction volume in a given year increases, the SEC will lower the fee rate because each transaction has to contribute less to the target collection amount."[162] Currently these fees are set at $18.40 per million dollars of trades.[163] Exchanges delegate the responsibility for fee collection to brokers, who then collect the fees from the investor, equaling a few pennies on each trade.

D. THE COSTS AND BENEFITS OF COMPLETELY REPLACING THE TRADITIONAL STOCK MARKET

There is no need to outlaw the traditional stock market in favor of a cryptosecurities market. A complete replacement is impractical and — due to institutional inertia — impossible unless Congress were to significantly

161. *About Settling Trades in Three Days: T+3*, SEC, http://www.sec.gov/investor/pubs/tplus3.htm (last updated May 21, 2004).

162. *"SEC Fee"—Section 31 Transaction Fees*, SEC, http://www.sec.gov/answers/sec31.htm (last updated Sept. 25, 2013).

163. Press Release, SEC, Fee Rate Advisory #4 for Fiscal Year 2015 (Feb. 27, 2015), http://www.sec.gov/news/pressrelease/2015-42.html.

rewrite the statutes governing securities laws. Many of the players in the traditional stock market would be displaced overnight, including transfer agents, brokers, and the traditional stock exchanges. Therefore, just as there is still a need for people to use the post office to send traditional email even though e-mail technology has been around for more than twenty years, it is unlikely that a cryptosecurities market will ever completely replace the traditional stock market.

V. REGULATING THE CRYPTOSECURITIES MARKET

Surprisingly, most of the existing regulatory framework would remain the same with a cryptosecurities market. The responsibilities and regulation of issuers, purchasers, or the exchanges would not change. One major change with a cryptosecurities market is that brokers will no longer be required to be involved in trades, leaving traders the ability to trade directly through the exchanges or peer-to-peer. Another major change involves the role of transfer agents — the Blockchain used in a cryptosecurities market would completely obviate the need for transfer agents.

A. BROKER-DEALERS

If I want to buy traditional stock listed on NASDAQ or the NYSE, I first would have to place an order through my broker.[164] My broker then would send the order to the exchange and the exchange matches the order with a willing seller. Then the exchange confirms the trade with my broker and my broker will alert me that the trade is complete. I have three days to send the money to my broker to pay for this trade, the broker pays my money to the seller, and then the seller will send the stock certificates (proof-of-ownership) to my broker. I can request the certificate from my broker, but it will likely cost extra money.

Anytime I buy or sell, I have to pay a commission to my broker. If I use a full-service brokerage, the commission could be as high as $300 for one trade.[165] If I go through a discount brokerage — i.e., I make my trade online through a broker's website without any interaction with an actual person—then the average fee is around $10 with some discount brokers

164. Example largely taken from LARRY HARRIS, TRADING AND EXCHANGES: MARKET MICROSTRUCTURE FOR PRACTITIONERS 14 (Oxford Univ. Press rev. ed. 2002).

165. Patrick Gleeson, *How Much is the Average Stock Brokers Commission?*, THE NEST, http://budgeting.thenest.com/much-average-stock-brokers-commission-31078.html (last visited May 25, 2015).

charging as low as $5 per trade.[166]

A cryptosecurities market would do away with the requirement that traders must go through brokers in order to complete trades. Of course, inexperienced traders may still use a broker for broker-assisted trades. However, traders should be able to purchase or sell their cryptosecurities directly on the exchanges or directly peer-to-peer. Traders who purchase on the exchanges will still need to pay a fee for every trade, but that fee will be significantly less than even the cheapest discount brokerage fee of $5.

Traders can also sell directly peer-to-peer on the Blockchain if they are able to find someone willing to buy or sell at the desired price. The only parties involved in this transaction would be the buyer, the seller, and the network users verifying the transaction. It may be difficult even on a cryptosecurities market for buyers and sellers to find each other without the traditional matchers — exchanges, market makers, or broker-dealers.

B. TRANSFER AGENTS

Transfer agents are the record keepers of the stock market, and even predate the SEC.[167] A transfer agent's role is to "record changes of ownership, maintain the issuer's security holder records, cancel and issue certificates, and distribute dividends."[168] There are 450 registered transfer agents in the U.S., managing "roughly 276 million shareholder accounts for about 1.5 million issuers."[169] Transfer agents are required to register with the SEC and are regulated by Section 17A(c) of the 1934 Exchange Act and SEC rules and regulations.[170] Transfer agents are not governed by the exchanges.[171]

A cryptosecurities market would obviate the need for transfer agents. Paper certificates will no longer be necessary to prove ownership — the Blockchain will maintain a clear and reliable record of who owns what. SEC Commissioner Luis Aguilar spoke of the transfer agents' "'unique

166. *A Quick Guide to Stock Broker Commissions*, WISE STOCK BUYER (May 31, 2012), http://www.wisestockbuyer.com/2012/05/guide-to-stock-broker-commissions/.

167. *Who is the STA?*, SECURITIES TRANSFER ASSOCIATION, INC., http://www.stai.org/who-is-the-sta.php (last visited May 25, 2015).

168. *Transfer Agents*, SEC, https://www.sec.gov/divisions/marketreg/mrtransfer.shtml (last updated June 24, 2010).

169. Sarah N. Lynch, *SEC Eyes Transfer Agents in New Front Against U.S. Stock Fraudsters*, REUTERS (Jan. 12, 2015, 4:57 AM), http://www.reuters.com/article/2015/01/12/us-sec-transferagents-insight-idUSKBN0KL0BD20150112.

170. *Id.*

171. If the transfer agent is a bank, it will also be regulated by the Comptroller of the Currency, the Federal Reserve System, and the Federal Deposit Insurance Corporation ("FDIC"). *Transfer Agents*, *supra* note 168.

position' to identify and prevent unregistered, restricted shares from being sold illegally."[172] However, using technology like Colored Coins, issuers will be able to add code on top of the underlying shares that automatically provides for the necessary restrictions. Unregistered securities can be coded as unregistered, shares with restrictions on resell can be coded with the exact resell restrictions so that there is no confusion on when the shareholder may sell the shares.

C. ISSUERS

Issuers will have enormous flexibility with cryptosecurities offerings. Issuers will be able to easily issue stocks, bonds, or other types of securities with technology such as Colored Coins adding code onto the base security to give it unique features. Issuers will also easily be able to enforce the 180-day lock-up period required for company insiders by adding on code that forbids transfers for 180 days. Likewise, if the issuer is engaging in a private offering, the issuer will be able to implement resell restrictions through code rather than relying on the transfer agent to create a legend written on a paper stock certificate.[173]

This will flow fairly seamlessly for new cryptosecurities offerings. But what about the situation where an issuer or its traders wish to convert traditional securities into cryptosecurities? If traders want to convert, then they should be able to subject to being fully informed of what the transfer may mean. Just because it is the same issuer and the securities may even have identical rights, the two systems are otherwise completely separate and will have different valuation. Overstock's traditional stock may be trading around $25[174] a share, while the separate cryptosecurities shares could be selling for $15. In effect, it is like two different classes of shares.

Due to these differences, issuers should be allowed to create new offerings of cryptosecurities but should not be able to convert its outstanding shares to cryptoshares without full approval from its existing shareholders. Otherwise it would be like converting preferred stock into common stock without permission, which is unacceptable. It is only the shareholders who are able to effectuate this conversion if they hold convertible preferred stock, and not the issuer. This concept should be used in the situation of converting traditional securities into

172. Lynch, *supra* note 169.

173. Although this paper focuses on public offerings, issuers engaging in private offerings could also use Blockchain technology to track the sale of private cryptosecurities. This will likely be my next paper topic.

174. $24.95 as of April 13, 2015. *Overstock.com, Inc.*, MARKETWATCH, http://www.marketwatch.com/investing/stock/ostk (last visited Apr. 13, 2015).

cryptosecurities and vice versa.

D. EXCHANGES

Long before traders made trades electronically or on the floor of a stock exchange, trades were completed outside in the open air.[175] Even as far back as 1788, traders would gather every day outside at what is now 68 Wall Street under a buttonwood tree to conduct their trades.[176] What would eventually become the New York Stock Exchange ("NYSE") eventually moved indoors in 1817, but traders continued to conduct business by the curbside.[177] As late as the Civil War, the majority of trades in the stock market were believed to have been conducted outside.[178]

Because the SEC has limited resources, it has delegated part of its regulatory function to the exchanges. The exchanges therefore play two roles: one as a publicly traded company in competition with other public companies; and the other role as a Self-Regulatory Organization ("SRO"). Stock exchanges enjoy certain immunity when acting in their role as SRO. As SROs, exchanges are responsible for regulating themselves (as evident by their name), their customers, and their competitors.

The exchanges' role as SRO should not greatly change with the advent of a cryptosecurities market. The traditional stock market is made up of public and private companies selling all manner of securities, whether through an exchange, over the counter, or directly. Many of these trades (see dark pools) happen outside the public eye, and only a portion of these trades happen on the exchanges. There will still be a need for stock exchanges to enable the buying and selling of cryptostock just like many Bitcoin users transfer on the Bitcoin exchanges rather than directly on the Blockchain.

Therefore, the exchanges will still play a role and their role and responsibilities with the SEC should remain largely the same, although parts of the exchanges' job will become automated with the Blockchain — e.g., specialists will likely play a much smaller role. More importantly, traders would not be required to go through a broker to effectuate trades, and could trade completely peer-to-peer. Traders should be able to log on

175. THE NEW YORK CURB MARKET: HISTORY, ORGANIZATION, LISTED AND UNLISTED REQUIREMENTS, EXECUTION OF AN ORDER, AMERICAN STOCK EXCHANGE 6 (3rd ed. 1928), http://babel.hathitrust.org/ cgi/pt?id=mdp.39015076045650;view=1up;seq=16.

176. *Id.*; Tom Miller, *The New York Curb Market Building—113–123 Greenwich Street*, DAYTONIAN IN MANHATTAN (Oct. 16, 2012, 2:48 AM), http://daytoninmanhattan.blogspot.com/2012 /10/the-new-york-curb-market-building-113.html.

177. *Id.*

178. *Id.*

to the exchange and trade their stock directly on the exchange, just as Bitcoin users are able to exchange Bitcoin directly on the exchanges.

There are two categories of exchanges capable of serving the cryptosecurities market in the near future. First are the national exchanges — such as NYSE and NASDAQ. These exchanges are in the best position to operate on the cryptosecurities market because they are well established, already have regulatory approval, and should be able to add on the necessary additional capacity.

Another category of exchanges that could transition to cryptosecurities is the existing Bitcoin exchanges, such as Coinbase[179] and Bitstamp.[180] Although these currency exchanges do not yet have the SEC regulatory approval, they do have experience with the Blockchain technology and how best to make Bitcoin transfers happen. Coinbase is the first U.S.-based licensed Bitcoin exchange, and it is actually backed by the NYSE.[181] With the support of the NYSE, I would argue that Coinbase is the top candidate for becoming a cryptosecurities exchange because it will bring to the table experience in both stock markets and cryptocurrency markets.

IV. CONCLUSION

Whether or not the stock market is broken, this article explores an alternative trading system that addresses several of the current problems with the traditional regime. Using Bitcoin's underlying technology — the Blockchain — issuers will be able to create cryptosecurities that will allow anyone in the public to be able to see each transaction as it is taking place, which will remove some of the shroud of secrecy surrounding much of the high frequency and dark pool trading occurring today. This alternative market will also allow traders to trade completely peer-to-peer or directly through an exchange — cutting out several layers of intermediaries including brokers and transfer agents. The key is that a cryptosecurities market would not require the replacement of the traditional stock market; rather it would be an alternative market for users dissatisfied with the current regime. It is likely there will always be a need for both systems, just as with the advent of email there is still a need for the post office to manage traditional letters.

179. COINBASE, https://www.coinbase.com (last visited Apr. 10, 2016).
180. BITSTAMP, https://www.bitstamp.net (last visited Apr. 10, 2016).
181. Bensinger, *supra* note 16.

VII. GLOSSARY OF BITCOIN TERMINOLOGY

51% attack	If more than 50% of the computing power (CPU) on the Bitcoin network is controlled by one miner or pool of miners, then that group could effectively hack into the Blockchain and rewrite the Blockchain's history.
Altcoin	Cryptocurrencies offered as an alternative to Bitcoin. Examples of popular altcoin include Ripple, NXT, Bitshares, and Ethereum.
Bitcoin	Bitcoin is the term to describe two separate concepts: (1) Bitcoin as the digital currency, and (2) Bitcoin as the entire network/protocol. Bitcoin is abbreviated as either BTC or XBT.
Bitcoin Address	A Bitcoin address is used to receive and send transactions on the Bitcoin network. It contains a string of alphanumeric characters, but can also be represented as a scannable QR code. The Bitcoin address is the only information that you need to give out in order for someone to pay you with Bitcoin. For security reasons, it is recommended that users create a new Bitcoin address per transaction.
Bitcoin Whitepaper	Satoshi Nakamoto authored "Bitcoin: A Peer-to-Peer Electronic Cash System" in November, 2008. This whitepaper lays out the fundamentals of the peer-to-peer network and the proof-of-work technology that would be implemented with the Bitcoin network.
BitPay	The most popular payment processor for Bitcoin. Merchants use BitPay to accept Bitcoin payments, using a scannable QR code.
Block	Blocks are like a page out of a ledger book, where the ledger is the Blockchain. Each block is connected to the previous block in order to form one long chain from the very first block (see genesis block) through the present day. Anywhere from hundreds to thousands of transactions will be entered and verified on a single block.
Blockchain	The Blockchain is the public ledger of every Bitcoin transaction ever made. It proceeds in chronological order from the very first Bitcoin block (see genesis block) through the present day. The Blockchain may be viewed by downloading the Bitcoin software or by

	viewing it online at blockchain.info. NOTE: Blockchain may also refer to the company that posts real-time Bitcoin transactions and is also a wallet software.
Block reward	This is the new Bitcoin creation reward that is given out to the miner who successfully adds a new block to the Blockchain. This reward started out at 50 Bitcoin, is currently at 25 Bitcoin, and will continue decreasing until all Bitcoin have been mined.
BTC	The currency abbreviation for bitcoins.
Client	See “miner.”
Confirmation	The process of successfully adding a new block to the Blockchain is called confirmation. Satoshi Nakamoto designed the system to take approximately ten minutes per block, with the difficulty level adjusting every two weeks to keep transaction times as close as possible to ten minutes.
Colored coins	Code added onto Bitcoins that create additional attributes, such as the ability to mark a particular Bitcoin as a stock or car. This allows users to trade Bitcoins as tokens for other property.
CPU	Stands for Central Processing Unit—the hardware on a computer. Today Bitcoin users typically must invest in something more powerful than a regular computer to do the mining work.
Coinbase transaction	This is another term for the Bitcoin reward that is released once a new block is successfully mined. Note: Coinbase is also the name of the first licensed U.S. Bitcoin exchange, backed by the NYSE.
Cryptocurrency	A type of currency that is completely digital and typically relies on cryptography in order to secure the system.
Cryptography	Cryptography is a type of mathematics involving codes and ciphers created in order to encrypt (secure) information. Cryptography is used in order to secure the Blockchain.
Cryptosecurity	Stocks and bonds that can be traded completely peer-to-peer and recorded on a public ledger for anyone to see.
Difficulty	Refers to the amount of effort that is required in order to add a new block to the Blockchain. Difficulty is

	automatically adjusted based on the amount of computational power devoted to solving the proof-of-work puzzle in order to keep transaction confirmation time at ten minutes.
Double Spending	Spending Bitcoins twice. This is possible if someone accepts a Bitcoin payment without waiting until the payment has been confirmed (ten minutes).
Elliptic Curve Cryptography	The Elliptic Curve Digital Signature Algorithm is the type of cryptography used to transform Private Keys into Public Keys. Abbreviated as ECDSA.
Exchange	A venue for exchanging one type of currency or asset for another.
Fiat Currency	Currency which derives its value from government regulation or law.
Fork	This occurs when a company creates a new cryptocurrency using the existing code of an established cryptocurrency. Namecoin is an example of the first cryptocurrency to create a fork from the Bitcoin Blockchain.
Genesis Block	The very first block in the block chain. This block does not contain any inputs (i.e. a hash from the previous block). Every other transaction leads back to the genesis block or to the coinbase transaction.
Hash	Used in cryptography to change an arbitrary input into a fixed output with certain properties. Because the output is meant to be random, it is almost impossible to determine what the original input was. Any change made to the input—even as small as change in capitalization or punctuation—will completely change the hash.
Input	The information on a Bitcoin transaction that shows where the Bitcoin came from. The public will only see the Bitcoin address.
Miner	This refers to the people—and their computers—who run the Blockchain. Also called a “node” or “client.” As a reward for devoting the computational effort required to verify transactions, Bitcoin miners are able to collect a transaction fee for each individual transaction that they confirm, and also receive a reward for each block that they successful add to the Blockchain.

Mining	The act of generating new Bitcoin by solving cryptographic problems using computing hardware.
Node	See "miner."
Nonce	A nonce is the proof string that miners search for when solving the proof-of-work puzzle. Miners will try billions of different nonces before discovering one that solves the puzzle. Once someone has figured out the nonce, it is much easier to verify that this is the correct solution, and the block that receives the most verification will be added to the Blockchain.
Orphan Block	A block that does not become valid on the Blockchain. Also called a "rejected block."
Output	Where the Bitcoin will be delivered.
Peer-to-Peer (P2P)	These are decentralized transactions that involve only the two parties in the transaction—the buyer and the seller. There are no third-party intermediaries (such as a bank) involved in peer-to-peer transactions.
Pool	A group of miners who collectively mine blocks and then split the reward between them.
Private Key	An alphanumeric string of data that proves that someone has the rights to the Bitcoin. Like cash, if someone loses their private key, their Bitcoin is gone forever. These are typically stored on a Bitcoin wallet, and it is recommended to store this information offline. Users should never reveal their private key to anyone. This is also used to sign transactions.
Proof-of-stake	An alternative to proof-of-work, in which your existing stake in a currency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine.
Proof-of-work	A system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof-of-work.
Public Key	An alphanumeric string of data that is derived from the private key, and once it goes through cryptographic hashing, will become that Bitcoin address that can be made available to the public.

Satoshi	The smallest unit of Bitcoin that may be transferred, equal to one millionth of a Bitcoin (0.00000001).
Satoshi Nakamoto	The name used by the original inventor of the Bitcoin. It is likely this name is a pseudonym for a person or group of individuals. During Bitcoin's first few years, Satoshi Nakamoto was active on blogs, but has not been heard from since 2010.
Satoshi Nakamoto Whitepaper	See Bitcoin Whitepaper.
Signature	Created by hashing private and public keys together in order to prove that a bitcoin transaction came from a particular address. This is required for every transfer of Bitcoin.
SHA-256	The cryptographic function that is used as the basis for the Blockchain.
Stale	Once a block has been successfully added to the system, any other efforts at mining that block become "stale." There is no reward associated with working on a stale block.
Ten Minute Transactions	The Bitcoin protocol is set to ensure ten minutes in between block confirmations. This is accomplished by adjusting the difficulty level once every two weeks. If transactions begin taking less than ten minutes to confirm, the difficulty level is adjusted upwards. Likewise, if transactions begin taking more than ten minutes, the difficulty level will be adjusted downward.
Transaction fee	A small fee imposed on Bitcoin transactions. Although this fee is not explicit, it is implied as the output will always equal a small amount less than the input. These fees are given to the miners who successfully confirm the transaction.
Wallet	Like a physical wallet, a Bitcoin wallet stores a person's Bitcoin for later use. It will also contain the private key, public key, and Bitcoin addresses that a user creates. Bitcoin wallets will display a user's total balance and allows users to designate specific amounts to send to another user.

THE BITCOIN BLOCKCHAIN AS FINANCIAL MARKET INFRASTRUCTURE: A CONSIDERATION OF OPERATIONAL RISK

*Angela Walch**

"Blockchain" is the word on the street these days, with every significant financial institution, from Goldman Sachs to NASDAQ, experimenting with this new technology. Many say that this remarkable innovation could radically transform our financial system, eliminating the costs and inefficiencies that plague our existing financial infrastructures, such as payment, settlement, and clearing systems. Venture capital investments are pouring into blockchain startups, which are scrambling to disrupt the "quadrillion"-dollar markets represented by existing financial market infrastructures. A debate rages over whether public, "permissionless" blockchains (like Bitcoin's) or private, "permissioned" blockchains (like those being designed at many large banks) are more desirable.

Amidst this flurry of innovation and investment, this Article inquires into the suitability of the Bitcoin blockchain to serve as the backbone of financial market infrastructure, and evaluates whether it is robust enough to serve as the foundation of major payment, settlement, clearing, or trading systems.

Positing a scenario in which the Bitcoin blockchain does serve as the technology enabling significant financial market infrastructures, this Article highlights the vital importance of functioning financial market infrastructure to global financial stability, and describes relevant principles that global financial regulators have adopted to help maintain this stability, focusing particularly on governance, risk management, and operational risk.

The Article then moves to explicate the operational risks generated by the most fundamental features of Bitcoin: its status as decentralized, open-source software. Illuminating the inevitable operational risks of software, such as its vulnerability to bugs and hacking (as well as Bitcoin's unique

* Assistant Professor, St. Mary's University School of Law. J.D., Harvard Law School, 2002. A.B., Harvard College, 1998. I would like to thank Michael Ariens, Shawn Bayern, Catherine Martin Christopher, Reuben Grinberg, Colin Marks, Eric Posner, Todd Senulis, Jonathan Zittrain, Paul Finkelman, the editors of the *New York Journal of Legislation & Public Policy*, participants at the "Inside Bitcoins NYC" conference from July 2013, participants in the 2014 Arizona State University Legal Scholars Conference, participants at the 2015 Harvard Law School Institute of Global Law and Policy mini-conference on Monetary Design in Global Perspective, and students in my Law of Money seminars for helpful comments, explanations, and insights. I would also like to thank my research assistants Tapash Agarwal, Sarah Scheidt, and Andrew Stephens. Finally, I am grateful for the support, sacrifice, and wisdom of my husband, Scott Russell.

"51% Attack" vulnerability), uneven adoption of new releases, and its opaque nature to all except coders, the Article argues that these technology risks are exacerbated by the governance risks generated by Bitcoin's ambiguous governance structure. The Article then teases out the operational risks spawned by decentralized, open-source governance, including that no one is responsible for resolving a crisis with the software; no one can legitimately serve as "the voice" of the software; code maintenance and repair may be delayed or imperfect because not enough time is devoted to the code by volunteer software developers (or, if the coders are paid by private companies, the code development may be influenced by conflicts of interest); consensus on important changes to the code may be difficult or impossible to achieve, leading to splits in the blockchain; and the software developers who "run" the Bitcoin blockchain seem to have backgrounds in software coding rather than in policy-making or risk management for financial market infrastructure.

The Article concludes that these operational risks, generated by Bitcoin's most fundamental, presumably inalterable, structures, strongly undermine the Bitcoin blockchain's suitability to serve as financial market infrastructure.

INTRODUCTION

We have elected to put our money and faith in a mathematical framework that is free of politics and human error . . . .

—Tyler Winkelvoss, as reported in the *New York Times*[1]

If no-one owns it, how can I trust it?

. . .

In short, if you trust mathematics, you can trust Bitcoin.

—Multibit.org[2]

There are places where authority is required: No one should want Congress's laws on a wiki. Or instructions for administering medication. Or the flight plan of a commercial airliner.

—Lawrence Lessig, *Remix: Making Art and Commerce Thrive in the Hybrid Economy*[3]

The faith that technology can redeem all of our sins and fix all of our problems is the ultimate hubris.

— Siva Vaidhyanathan, *The Googlization of Everything*[4]

Working on Bitcoin's core code is really scary, actually, because if you wreck something, you can break this huge $8 billion project. . . . And that's happened. We have broken it in the past.

—Gavin Andresen, Bitcoin core developer, as reported in *Newsweek*[5]

Since 2012, almost $930 million of venture capital has been invested in virtual currency companies,[6] with over $450 million invested

---

1. Nathaniel Popper & Peter Lattman, *Never Mind Facebook; Winklevoss Twins Rule in Digital Money*, N.Y. TIMES, April 11, 2013, at A3 (quoting a statement by Tyler Winklevoss).

2. *Frequently Asked Questions*, MULTIBIT, https://multibit.org/faq.html (last visited Oct. 21, 2015). Multibit is a Bitcoin wallet. Companies that store Bitcoin users' private keys (essentially passwords), which enable them to transfer their bitcoins, are known as "wallet" companies.

3. LAWRENCE LESSIG, REMIX: MAKING ART AND COMMERCE THRIVE IN THE HYBRID ECONOMY 85 (2008).

4. SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY) 77 (updated ed. 2011).

5. Leah McGrath Goodman, *The Face Behind Bitcoin*, NEWSWEEK, Mar. 14, 2014, at 21 (quoting Gavin Andresen, core developer of the Bitcoin software code).

6. *See Bitcoin Venture Capital*, COINDESK, http://www.coindesk.com/bitcoin-venture-capital/ (last visited Oct. 22, 2015).

in 2015 alone.[7] In the past eighteen months, a former Chairman of the Securities and Exchange Commission,[8] a former Treasury Secretary and chief economic advisor of President Obama,[9] a former chair of the Federal Deposit Insurance Corporation (FDIC),[10] and a former CEO of the Depository Trust and Clearing Corporation (DTCC)[11] have become advisors to or board members of virtual currency companies. Richard Branson has thrown an exclusive invitation-only "blockchain" summit on his private island,[12] and elite universities like Stanford and MIT are offering courses on virtual currencies.[13]

"Blockchain"[14] is the buzzword of the moment in financial circles, with a debate raging over whether private (permissioned) blockchains or public (permissionless) blockchains are more desirable for financial structures.[15] Some businesses are building their own pri-

---

7. *See id.*

8. *See Arthur Levitt Advises Bitcoin Companies: BitPay and Vaurum*, BUSINESSWIRE (Oct. 28, 2014), http://www.businesswire.com/news/home/20141028005244/en/Arthur-Levitt-Advises-Bitcoin-Companies-BitPay-Vaurum#.Vgye8ctViko (reporting that Arthur Levitt, former chairman of the Securities and Exchange Commission, will serve as an advisor to BitPay (a Bitcoin payment processor) and Vaurum (a Bitcoin exchange)).

9. *See* Michael Casey, *Bitcoin Startup 21 Unveils Product Plan: Embeddable Mining Chips*, DOW JONES INST. NEWS (May 18, 2015) (reporting that Lawrence Summers, former Secretary of the Treasury, has joined the advisory board of 21 Inc., a Bitcoin company seeking to produce an "embedded mining chip"); Yessi Bello Perez, *Xapo Adds Former Visa and Citibank Execs to Board of Advisors*, COINDESK (May 26, 2015), http://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/ (reporting that Summers had been appointed to the board of advisors of Xapo, a Bitcoin services provider, along with the founder of Visa and the former CEO of Citibank).

10. *See* Nathaniel Popper, *ItBit Bitcoin Exchange Gets Banking License in New York, A First in U.S.*, N.Y. TIMES, May 8, 2015, at B5 (reporting that Sheila Bair, former chairwoman of the Federal Deposit Insurance Corporation, had been appointed a board member of ItBit, a Bitcoin exchange).

11. Yessi Bello Perez, *Ripple Appoints DTCC's Former CEO as Advisor*, COINDESK (June 1, 2015), http://www.coindesk.com/ripple-appoints-dtccs-former-ceo-as-advisor/ (reporting that Donald Donahue, former CEO of the Depository Trust & Clearing Corporation (DTCC), "the main clearinghouse for US securities and derivatives," became an advisor to Ripple Labs, a digital currency company).

12. *See* BLOCKCHAIN SUMMIT, http://www.blockchainsummit.io/ (providing information on the May 25–28, 2015 Blockchain Summit held on Necker Island).

13. *See* Danielle Meegan, *The New Virtual Currency Trend: Going Back to School!*, DIGITAL MONEY CORP. (Sept. 15, 2015), http://www.digitalmoneycorp.com/blog/the-new-virtual-currency-trend-going-back-to-school/ (reporting that universities such as MIT, Stanford, NYU, Princeton, and Duke offer courses on virtual currencies).

14. "Blockchain" is the word for the common ledger, or list, that is maintained by virtual currencies. In Part I, I provide an overview of how Bitcoin and its blockchain operate.

15. Private (permissioned) blockchains are common ledgers shared amongst a known group of parties with only certain parties having the ability, or permission, to

vate blockchains, while others are building on top of the Bitcoin blockchain.[16] In this Article, I consider the implications of building financial market infrastructure[17]—such as payment, settlement, or clearing systems—on top of the Bitcoin blockchain. I do this from an operational risk perspective, examining how Bitcoin's most fundamental features—its status as decentralized, open-source software—

make changes to the ledger. Public (permissionless) blockchains like Bitcoin's are publicly available common ledgers that allow anyone who runs the Bitcoin software to participate in making changes to the ledger. *See* BitFury Grp. & Jeff Garzik, Public Versus Private Blockchains: Part I: Permissioned Blockchains (2015), http://bitfury.com/content/4-white-papers-research/public-vs-private-pt1-1.pdf (presenting an explanation of permissioned and permissionless blockchains, and arguments for and against each type, focusing on the Bitcoin blockchain as "the most commercially successful and secure permissionless blockchain"); BitFury Grp. & Jeff Garzik, Public Versus Private Blockchains: Part II: Permissionless Blockchains (2015) (same); Ian Allison, *Nick Szabo: If Banks Want Benefits of Blockchains They Must Go Permissionless*, Int'l Bus. Times (Sept. 8, 2015), http://www.ibtimes.co.uk/nick-szabo-if-banks-want-benefits-blockchains-they-must-go-permissionless-1518874 (reporting on an interview with cryptography and cyber expert Nick Szabo, who argued that permissionless blockchains offer true innovation while permissioned blockchains keep existing problems with financial infrastructures); Giulio Prisco*, Blythe Masters and Wall Street Opt for 'Permissioned' Non-Bitcoin Blockchains*, Bitcoin Mag. (Sept. 2, 2015), https://bitcoinmagazine.com/articles/blythe-masters-wall-street-opt-permissioned-non-bitcoin-blockchains-1441227797 (reporting that permissioned blockchains are attractive to companies because they offer "a completely known universe of transaction processors").

16. *See* Prisco, *supra* note 15 (reporting that many financial institutions are working to create private blockchains rather than relying on the Bitcoin blockchain); Andrew Robinson & Matthew Leising, *Blythe Masters Tells Banks: The Blockchain Changes Everything*, Bloomberg (Aug. 31, 2015), http://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything (noting that NASDAQ is using the Bitcoin blockchain to trial certain share issuances and transfers).

17. Although Bitcoin is not now functioning as financial market infrastructure, in this Article I consider the implications of the Bitcoin blockchain potentially *supporting* financial market infrastructure. I therefore use the Federal Reserve's definition of "financial market infrastructures," which is consistent with the definition used globally, throughout this Article. *See Supervision and Oversight of Financial Market Infrastructures*, Fed. Res. (Sept. 2, 2009), http://www.federalreserve.gov/paymentsystems/over_about.htm. The Federal Reserve defines "financial market infrastructures" as "multilateral systems among participating financial institutions, including the system operator, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions." *Id.* These infrastructures, also referred to as FMIs, "include payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories." *Id.*; *see also* Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. 67,326, 67,333 (Nov. 12, 2014); Comm. on Payment & Settlement Sys. & Tech. Comm. of the Int'l Org. of Sec. Comm'ns, Principles for Financial Market Infrastructures (2012), www.bis.org/cpmi/publ/d101a.pdf [hereinafter PFMI] (upon which the Federal Reserve's definition of financial market infrastructure is based).

pose important risks to its stability as potential financial market infrastructure.

In Parts I and II of the Article, I provide needed context for the reader. Part I provides a brief overview of the key features of Bitcoin and its blockchain that are relevant to my argument. Part II discusses how Bitcoin and blockchain technology are poised to disrupt financial market infrastructures, why the uninterrupted operation of these systems is so vital, and how global financial regulators address operational risks[18] in existing financial market infrastructures.

Part III provides the meat of my argument. In this Part, I lay out the operational risks of Bitcoin that concern me, including the inherent vulnerabilities of software, the governance problems that arise from Bitcoin's decentralized, open-source status, and the expertise problems that stem from having software developers control potential financial market infrastructure through their code development. After explaining each risk, I demonstrate how each threatens the Bitcoin blockchain's reliability as potential financial market infrastructure. In Part IV, I provide possible reasons why these operational risks have not received as much regulatory or academic attention as the "use" risks of Bitcoin.[19]

I conclude the Article with recommendations that policy-makers, regulators, and the business community explicitly factor these risks into their evaluation of the Bitcoin blockchain (and that of other virtual currencies) as potential financial market infrastructure. I also briefly outline the larger questions that my analysis raises about the use of open-source software in other critical infrastructures.

Before jumping in, it may be helpful to clarify what I am *not* doing in this Article. In considering the operational risks of Bitcoin in

---

18. In the Federal Reserve Policy on Payment System Risk, the Federal Reserve defines "operational risk" as "the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the FMI." Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. at 67,334. Furthermore, the policy states that operational risk "includes physical threats, such as natural disasters and terrorist attacks, and information security threats, such as cyberattacks. Further, deficiencies in information systems or internal processes include errors or delays in processing, system outages, insufficient capacity, fraud, data loss, and leakage." *Id.* at 67,334 n.8. The policy notes that this definition of operational risk is "consistent with [that] presented in the PFMI." *Id.* at 67,334 n.6. I use this definition throughout this Article.

19. I consider the "use" risks of Bitcoin to be those risks that arise from how it may be used, such as crimes that can be committed with it (like money laundering and online sales of illegal goods and services), how it should be taxed, how people who handle it on behalf of others (e.g., exchanges and wallet companies) should be regulated, etc.

connection with its blockchain's suitability as financial market infrastructure, I am not defending existing financial market infrastructures as flawless, or even necessarily better than the Bitcoin blockchain.[20] For instance, this Article is not intended to be a defense of the costly and slow existing payment systems. It may be that after a weighing of risks and benefits, financial systems that run on the Bitcoin blockchain (or that of other decentralized virtual currencies) are more desirable than certain existing financial market infrastructures. However, I want to be sure that we are adequately considering Bitcoin's operational risks (primarily stemming from technology and governance issues) in performing the cost-benefit analysis, and below, I seek to flesh out those risks.

My primary goal in this Article is to ensure that the cost-benefit analysis performed in determining whether to replace existing financial market infrastructure with systems built on top of the Bitcoin blockchain is as fulsome as possible—explicitly accounting for operational risks. Infrastructure's most essential trait is *reliability*, and thus evaluating the reliability of potentially new infrastructure must be done with great care.

I.
Bitcoin and Its Blockchain

Bitcoin is peer-to-peer[21] open-source[22] software that operates to create and maintain a distributed public ledger.[23] This public ledger is

---

20. Existing financial market infrastructures are known to be costly and inefficient. *See* Robinson & Leising, *supra* note 16 (describing the "opaque and clunky back-office processes" that slow financial transactions).

21. Peer-to-peer software is distinctive in that a central computer server does not run it. Rather, the software operates over the connections that individual computers make with one another. For an overview of peer-to-peer software, see Detlef Schoder, Kai Fischbach & Christian Schmitt, *Core Concepts in Peer-to-Peer Networking*, *in* Peer to Peer Computing: The Evolution of a Disruptive Technology 1–27 (Ramesh Subramanian & Brian D. Goodman eds., 2005).

22. For a sustained discussion of open-source software, see *infra* Part III.C.

23. *See* Andreas M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies 18 (2014). Mr. Antonopoulos is a well-respected figure in the Bitcoin community and has taught university courses on digital currencies. I have chosen to cite his December 2014 book on Bitcoin for many of the basics of Bitcoin's operation because he is an identifiable, seemingly credible person, while the website that purports to be "behind" Bitcoin (bitcoin.org) does not come from a unified, identifiable source. *See About Bitcoin.org: Who Owns Bitcoin.org?*, Bitcoin.org, https://bitcoin.org/en/about-us (last visited Oct. 21, 2015) ("Bitcoin.org was originally registered and owned by Bitcoin's first two developers, Satoshi Nakamoto and Martti Malmi. When Nakamoto left the project, he gave ownership of the domain to additional people, separate from the Bitcoin developers, to spread responsibility and prevent any one person or group from easily gaining control over the Bitcoin project. . . .

known as the "blockchain,"[24] and it is analogous to a database that shows all changes made since its creation. The Bitcoin blockchain is maintained by a network of computers (referred to as "miners") that solves complex mathematical equations as part of verifying changes made to the ledger.[25] Crucially, the network of computers running the Bitcoin software and maintaining the blockchain is *decentralized*, with no central authority that controls it.[26] Because there are no permissions required to join the network of computers that run the Bitcoin software and help to maintain the blockchain, the Bitcoin blockchain is said to be public, or "permissionless," distinguishing it from private, or "permissioned," blockchains that are being developed by financial and technology companies.[27]

Major players in the financial industry have seized on the technology that maintains the blockchain (or common ledger) as a significant innovation.[28] It is seen as a way to achieve a reliable shared list without having a central party to maintain it.[29]

Importantly, the computer network that runs the Bitcoin software is not the only part of Bitcoin that is decentralized. The software development process is as well, meaning that there is no central entity that is officially charged with maintaining or fixing the software.[30] In fact, the actual creator of the Bitcoin software remains a mystery; an unknown software coder or group of coders known by the pseudonym "Satoshi Nakamoto" introduced it to the world in 2009.[31]

The Bitcoin software has evolved significantly since its initial release,[32] and changes to the software have come about through the

---

Bitcoin.org is not Bitcoin's official website. Just like nobody owns the email technology, nobody owns the Bitcoin network. *As such, nobody can speak with authority in the name of Bitcoin.*" (emphasis added)).

24. *See* ANTONOPOULOS, *supra* note 23, at 176–77.

25. *Id.* at 173–74.

26. *See id.* at 1.

27. *See supra* notes 15–16 and accompanying text.

28. *See, e.g.*, Nathaniel Popper, *Wall Street Takes a Keen Interest in Bitcoin's Latest Technology; Bitcoin's Blockchain Tech Is Being Examined to See if It Can Be Used to Create a New Way of Transacting Online*, IRISH TIMES (Sept. 14, 2015), http://www.irishtimes.com/business/wall-street-takes-a-keen-interest-in-bitcoin-s-technology-1.2340274 (reporting on the interest in blockchain technology by numerous major banks across the globe).

29. *See id.*; Robinson & Leising, *supra* note 16; *The Great Chain of Being Sure About Things*, ECONOMIST, Oct. 31, 2015, at 21.

30. *See* ANTONOPOULOS, *supra* note 23, at 1.

31. *See id.* at 3–4.

32. *See* Goodman, *supra* note 5, at 23 (quoting Gavin Andresen, head developer of the Bitcoin software code, as stating that the developers "have rewritten roughly 70 percent of the code since inception").

efforts of a mix of volunteer and paid programmers, who determine what changes should be made through "informal processes that depend on rough notions of consensus and that are subject to no fixed legal or organizational structure."[33] As will be discussed at length in this Article, Bitcoin software maintenance and development are spearheaded by a team of around five "core developers,"[34] who release periodic new versions of the software,[35] and who have certain privileges that other coders do not, such as the ability to send emergency messages to all nodes[36] and to make decisions about what changes are included in a new release of the Bitcoin software.[37]

Although this Article focuses on the Bitcoin blockchain because that is the current topic of public conversation, Bitcoin was initially seen as a possible alternative currency and is often referred to as a virtual currency, digital currency, or cryptocurrency.[38] There have

33. Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. U. L. REV. ONLINE 257, 259 (2014).

34. The core developers listed on the Bitcoin software development website are Wladimir J. van der Laan, Gavin Andresen, Jeff Garzik, Gregory Maxwell, and Pieter Wuille. *Bitcoin Development*, BITCOIN.ORG, https://bitcoin.org/en/development (last visited Nov. 14, 2015).

35. *See, e.g.*, Joon Ian Wong, *Bitcoin Core 0.10 Gives Developers Simplified Access to Network Consensus*, COINDESK (Feb. 17, 2015), http://www.coindesk.com/bitcoin-core-0-10-gives-developers-simplified-access-network-concensus/ (reporting on the February 16, 2015 release of core Bitcoin software by the core developers).

36. The emergency message power "allow[s] the core developer team to notify all bitcoin users of a serious problem in the bitcoin network, such as a critical bug that require[s] user action." ANTONOPOULOS, *supra* note 23, at 157. Alerts have "only been used a handful of times, most notably in early 2013 when a critical database bug caused a multiblock fork to occur in the bitcoin blockchain." *Id.* The password that allows the sending of the network-wide emergency messages is held only "by a few select members of the core development team." *Id.*; *see also* ARTHUR GERVAIS ET AL., IS BITCOIN A DECENTRALIZED CURRENCY? (2014), http://eprint.iacr.org/2013/829.pdf (arguing that giving the emergency alert power only to the core developers "gives these entities privileged powers to reach out to users and urge them to adopt a given Bitcoin release").

37. *See* Tom Simonite, *The Man Who Really Built Bitcoin*, MIT TECH. REV. (Aug. 15, 2014), http://www.technologyreview.com/featuredstory/527051/the-man-who-really-built-bitcoin/ (describing how only the core developers have the power to "change the code behind Bitcoin and merge in proposals from other volunteers"); *see also* GERVAIS ET AL., *supra* note 36, at 6 ("This [software development process] limits the impact that users have, irrespective of their computing power, to affect the development of the official Bitcoin [software].").

38. Regulators have sought in recent years to create a definition of "virtual currency." In 2012, the European Central Bank (ECB) defined "virtual currency" as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community." EUROPEAN CENT. BANK, VIRTUAL CURRENCY SCHEMES 5 (2012), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [hereinafter 2012 ECB PAPER]. In 2015, the ECB revised its definition of "virtual currency" to "a

been prior attempts to create virtual currency, or digital money,[39] but Bitcoin is the most successful thus far.[40] In the context of Bitcoin as a virtual currency, the currency unit is described as a "bitcoin."[41] A "bitcoin" is actually only an entry within the blockchain, marking a party's right to spend a certain amount of bitcoins.[42] There is no actual file or other tangible "thing" that comprises a bitcoin—it is just a representation of ownership within the blockchain.[43] When a bitcoin is transferred to another party, all the computers that run the Bitcoin software (referred to as "nodes") work together to verify that the party seeking to transfer that bitcoin has not already transferred it to someone else.[44] This prevents double-spending of a bitcoin by its owner.[45]

As of this writing, there are nearly fifteen million bitcoins in circulation;[46] the software caps the total number of bitcoins ever to be created at twenty-one million.[47] New bitcoins are created through the blockchain verification process, with the first computer to solve the equations that verify transactions compensated with a specified num-

---

digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money." EUROPEAN CENT. BANK, VIRTUAL CURRENCY SCHEMES: A FURTHER ANALYSIS 25 (2015), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf [hereinafter 2015 ECB PAPER]. The U.S. Department of the Treasury has defined "virtual currency" as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency." DEP'T OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, FIN-2013-G0001, Application of FinCENS's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies 1 (2013). The U.S. Government Accountability Office (GAO) defines "virtual currency" as "a digital representation of value that is not government-issued legal tender." *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-496, VIRTUAL CURRENCIES: EMERGING REGULATORY, LAW ENFORCEMENT, AND CONSUMER PROTECTION CHALLENGES 4 (2014).

39. *See* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 168–74 (2012) (providing a historical overview of prior forms of digital or virtual currencies).

40. *See* 2015 ECB PAPER, *supra* note 38, at 6–7.

41. A convention has developed to distinguish between (a) references to the Bitcoin software and network and (b) references to individual bitcoins that comprise the units of the currency. Lower case "bitcoins" refer to the individual units of the currency; upper case "Bitcoin" refers generally to the phenomenon of Bitcoin, the software, its protocol, or the Bitcoin network. *See Vocabulary,* BITCOIN.ORG, https://bitcoin.org/en/vocabulary.

42. *See* 2015 ECB PAPER, *supra* note 38, at 13 ("[U]sers do not hold units of the currency in decentralised [virtual currencies]. They actually hold keys which give access to a certain account balance, which is stored in the blockchain.").

43. *See id.*

44. *See* ANTONOPOULOS, *supra* note 23, at 109–11.

45. *See id.*

46. *Total Bitcoins in Circulation*, BLOCKCHAIN, https://blockchain.info/charts/total-bitcoins (last visited Oct. 22, 2015).

47. *See* ANTONOPOULOS, *supra* note 23, at 2.

ber of newly created bitcoins.[48] This compensation incentivizes parties to participate in the Bitcoin network and ensures that the blockchain is maintained. By design, the pace of mining bitcoins becomes slower and slower, as over time the difficulty of the equations to be solved by the miners increases while the number of bitcoins awarded for solving equations decreases.[49] Although individuals started out as the initial miners of bitcoins, as mining began to be seen as lucrative, an arms race of sorts developed to generate bitcoins the fastest.[50] This has culminated in extremely high-powered and expensive computer equipment, coupled with vast amounts of electricity, being needed to mine bitcoins. As a result, mining is now almost exclusively dominated by businesses devoted to mining and mining consortiums (known as "pools").[51]

For my purposes, what is most important about Bitcoin is that many people believe that its blockchain innovation can disrupt important systems within our society, including systems that comprise our financial market infrastructures.[52] In Part II, I discuss this possible disruption and how global financial regulators address operational risk in existing financial market infrastructures. Note that a detailed understanding of the Bitcoin software is unnecessary to follow the arguments made in this Article;[53] rather, the most basic attributes of Bitcoin are my focus: its status as *open-source, decentralized software* that purports to displace financial market infrastructures.

---

48. *Id.* at 173.

49. *See id.* at 195–96.

50. *See id.* at 204–06. For an analysis of Bitcoin mining practices, see generally NICOLAS T. COURTOIS ET AL., THE FUNDAMENTAL INCERTITUDES OF BITCOIN MINING (3d ed. 2014), http://arxiv.org/pdf/1310.7935v3.pdf.

51. *See* ANTONOPOULOS, *supra* note 23, at 207–10.

52. *See, e.g.*, ACCENTURE, BLOCKCHAIN IN THE INVESTMENT BANK 5 (2015), http://fsblog.accenture.com/capital-markets/wp-content/uploads/sites/2/2015/06/CM_ATS_POV_Blockchain_in_the_Investment_Bank-web.pdf ("Accenture believes that, although the potential of the technology is only just emerging, Blockchains will become the critical backbone of the future capital markets infrastructure."); Laura Shin, *Money's New Operating System*, FORBES, Sept. 28, 2015, at 100 (reporting on the ways that blockchains may alter existing financial and recordkeeping practices); Robinson & Leising, *supra* note 16 (reporting claims that blockchains will be as transformative as the Internet toward financial systems).

53. For a more substantial technical description of Bitcoin, see generally ANTONOPOULOS, *supra* note 23 (providing a useful overview of how Bitcoin works by a prominent Bitcoin proponent and directed primarily at software coders). For cultural analyses of the phenomenon, see generally NATHANIEL POPPER, DIGITAL GOLD: BITCOIN AND THE INSIDE STORY OF THE MISFITS AND MILLIONAIRES TRYING TO REINVENT MONEY (2015) (providing a history of Bitcoin and the people involved with it); PAUL VIGNA & MICHAEL J. CASEY, THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER (2015) (providing an overview of Bitcoin along with the risks and opportunities it presents).

II. Disrupting Existing Financial Market Infrastructures

As discussed above, the proponents of Bitcoin and other virtual currencies seek to replace existing financial market infrastructures. In this Part, I discuss this potential disruption, the significance of financial market infrastructure, and how global financial regulators address operational risk in existing financial market infrastructures.

A. *Virtual Currency as Disruptor*

The name of the game with virtual currency is disruption. Proponents of Bitcoin and blockchain technology speak of the quadrillion-dollar markets they seek to displace.[54]

In the early days of Bitcoin, the buzz was primarily about how Bitcoin could serve as an actual currency that displaced the fiat currencies issued by governments.[55] When the economy of Cyprus collapsed in 2013, the price of Bitcoin spiked as many depositors in Cypriot banks bought bitcoins to avoid having government currency that could be frozen or seized by the government.[56] Many of the early users of Bitcoin were motivated by the idea of the creation of money moving from the hands of government to the hands of individuals.[57]

In the intervening years, many economists and finance scholars have critiqued Bitcoin's capacity to serve as money. They have noted that Bitcoin fails to perform the three basic functions of money (to serve as a unit of account, a store of value, and a medium of exchange) due to the extreme swings in its value and the limited number of parties that will accept it.[58] Others have pointed to flaws in the

---

54. *See Consensus*, 10TIMES.COM, http://10times.com/consensus-newyork (last visited Nov. 18, 2015) (describing a blockchain conference, sponsored by prominent virtual currency news site CoinDesk, in which one of the panels discussed the opportunity for blockchain technology to disrupt the $1.6 quadrillion securities settlement and clearing market).

55. *See, e.g.*, David Yermack, *Is Bitcoin a Real Currency? An Economic Appraisal* 7–8 (Nat'l Bureau of Econ. Research, Working Paper No. 19747, 2014).

56. *See* Emma Rowley, *Russians Most Interested in Bitcoin, Searches Show*, SUNDAY TELEGRAPH (Apr. 6, 2013), http://www.telegraph.co.uk/finance/economics/9976524/Russians-most-interested-in-Bitcoin-searches-show.html (reporting speculation that Bitcoin's price increase was related to the Cyprus banking crisis).

57. *See, e.g.*, Grinberg, *supra* note 39, at 172–74 (describing the attraction that Bitcoin holds for "gold bugs"); Yermack, *supra* note 55, at 7–8 (describing the libertarian interest in Bitcoin "due to its lack of connection to any government").

58. *See, e.g.*, 2015 ECB PAPER, *supra* note 38, at 23–25 (noting that virtual currencies like Bitcoin are not money or currency from an economic or legal perspective); STEPHANIE LO & J. CHRISTINA WANG, FED. RESERVE BANK OF BOS., BITCOIN AS

monetary policy that is embedded in Bitcoin's structure, such as the hardwired limit on the number of bitcoins that may ever be created.[59] It seems that many have moved on from the idea that Bitcoin will be a viable currency that competes with government-issued currencies.[60]

More recently, the conversation about virtual currencies has shifted to a focus on the possible transformative applications of the blockchain—the common ledger that is verified through a decentralized computer network rather than by a single central party.[61] Prominent actors such as Andrew Haldane, Chief Economist of the Bank of England, and the Financial Stability Oversight Council have noted that Bitcoin and other virtual currencies may have promise as payment systems.[62] Others point to its ability to disrupt other aspects of the

---

MONEY? 3–11 (2014), https://www.bostonfed.org/economic/current-policy-perspectives/2014/cpp1404.pdf (concluding that Bitcoin does not perform money's functions as a medium of exchange, unit of account, or store of value); Yermack, *supra* note 55 (concluding that Bitcoin does not satisfy the standard definition of a currency because it does not perform money's functions as a medium of exchange, store of value, and unit of account); GOLDMAN SACHS GRP., ALL ABOUT BITCOIN 6 (2014), http://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf ("[B]itcoin, and other digital currencies, currently lie somewhere on the boundaries between currency, commodity and financial asset.").

59. *See, e.g.*, Paul Krugman, Opinion, *Golden Cyberfetters*, N.Y. TIMES (Sept. 7, 2011), http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/ (noting that Bitcoin is prone to deflation due to the limits on its quantity); Yermack, *supra* note 55, at 17 (arguing that Bitcoin is prone to deflation due to a cap on the number of bitcoins to be created); Daniel Reber & Simon Feurstein, *Bitcoins: Hype or Real Alternative*, *in* INTERNET ECONOMICS VIII, at 90 (Burkhard Stiller et al. eds., 2014) (noting that Bitcoin is subject to deflation in the long run).

60. *See Blockchain's Whirlwind Month—So Far*, PYMNTS.COM (Oct. 16, 2015), http://www.pymnts.com/in-depth/2015/blockchains-whirlwind-month-so-far/ (noting the shift in focus toward the potential of Bitcoin's blockchain technology rather than as a currency).

61. For recent feature articles on the blockchain in prominent financial publications, see, for example, Robinson & Leising, *supra* note 16; Shin, *supra* note 52; *The Great Chain of Being Sure About Things*, *supra* note 29; Jane Wild et al., *Technology: Banks Seek the Key to the Blockchain*, FIN. TIMES (Nov. 1, 2015).

62. *See, e.g.*, Andrew Haldane, Chief Economist of the Bank of Eng., Speech at the Portadown Chamber of Commerce: How Low Can You Go? (Sept. 18, 2015), http://www.bankofengland.co.uk/publications/Documents/speeches/2015/speech840.pdf (noting, in a speech about money and monetary policy, that "the distributed payment technology embodied in Bitcoin has real potential"); FIN. STABILITY OVERSIGHT COUNCIL, 2015 ANNUAL REPORT 114 (2015), http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf ("[T]he potential applications and uses of the peer-to-peer network for transferring value in the payment and financial service industry warrant continued monitoring."); Robleh Ali et al., *Innovations in Payment Technologies and the Emergence of Digital Currencies*, 54 BANK ENG. Q. BULL. 262, 266 (2014) (evaluating the promise that digital currencies hold for payment systems).

financial system.[63] Most of the largest financial institutions now have substantial teams of people devoted to investigating ways that blockchain technology could improve their businesses.[64] And titans of the finance and business world, from Larry Summers to Marc Andreessen, are rushing to become involved in virtual currencies.[65] Rather than being seen as a way to rebel against government-controlled currency, or a way to commit crime via the Internet, virtual currencies are now being viewed by regulators and financial industry stalwarts as a significant innovation for the financial system that could save time, cut costs, and create jobs.[66]

B. Regulatory Treatment of Existing Financial Market Infrastructures

This all sounds great. Don't we want to save time, cut costs, and create jobs every time there is an opportunity to do so? Isn't this a no-brainer?

It *is* good news that there is a new technology that could positively transform these areas. There are profuse criticisms of existing financial market infrastructures. Existing systems are faulted for their ancient and creaky technology, the slow speed at which payments are processed across borders or transactions are settled, and the high fees charged to move money around the world.[67] These systems feel obsolete in a world that is used to sending photos, videos, and other information via the swipe of a smartphone. The centralization and concentration of risk in large clearinghouses or settlement systems is also troubling to many.[68]

---

63. *See generally, e.g.*, Robinson & Leising, *supra* note 16; Shin, *supra* note 52; *The Great Chain of Being Sure About Things*, *supra* note 29; Wild et al., *supra* note 61.

64. *See* Wild et al., *supra* note 61 (describing the initiatives at major banks to investigate how the blockchain could be used to improve the financial services industry).

65. *See* Casey, *supra* note 9 (describing Lawrence Summers's involvement with virtual currency companies); *see also* Marc Andreessen, Opinion, *Why Bitcoin Matters*, N.Y. TIMES (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/ (comparing Bitcoin to the Internet in terms of its revolutionary potential).

66. For such claims by the financial industry, *see*, for example, *The Great Chain of Being Sure About Things*, *supra* note 29, at 24 (noting claims by Santander, a bank, that distributed ledgers could save the banking industry $20 billion a year by 2022); *see also* Robinson & Leising, *supra* note 16; Shin, *supra* note 52; Wild et al., *supra* note 61.

67. *See* Robinson & Leising, *supra* note 16; Shin, *supra* note 52.

68. *See generally, e.g.*, Felix B. Chang, *The Systemic Risk Paradox: Banks and Clearinghouses Under Regulation*, 2014 COLUM. BUS. L. REV. 747; Sean J. Griffith,

It should come as little surprise, then, that potential transformations in these areas are heralded as a big deal. But in all the excitement over this technological boon, we must keep in mind the enormous importance of reliable financial market infrastructure, and ensure that replacements to existing financial market infrastructures can be counted on. In the following paragraphs, I describe how global financial regulators treat existing financial market infrastructures. This discussion is not intended to be an in-depth treatise on the global regulation of financial market infrastructures, but rather a high-level overview. My goal here is to highlight the important role that financial market infrastructures are acknowledged to play in global financial stability, buttressing my argument that the operational risks of Bitcoin are relevant in evaluating its quality as potential financial market infrastructure.

First, what is "financial market infrastructure" and why is it of concern to global financial regulators? The Federal Reserve, consistent with standards set by the G20 and Financial Stability Board,[69] defines "financial market infrastructures" (or FMIs) as "multilateral systems among participating financial institutions, including the system operator, used for the purposes of clearing, settling, or recording

---

Governing Systemic Risk: Towards a Governance Structure for Derivatives Clearinghouses, 61 EMORY L.J. 1153 (2012); Kristin N. Johnson, *Clearinghouse Governance: Moving Beyond Cosmetic Reform*, 77 BROOK. L. REV. 681 (2012); Jeremy C. Kress, *Credit Default Swaps, Clearinghouses, and Systemic Risk: Why Centralized Counterparties Must Have Access to Central Bank Liquidity*, 48 HARV. J. ON LEGIS. 49 (2011).

69. Guido Ferrarini & Paolo Saguato, *Regulating Financial Market Infrastructures*, *in* OXFORD HANDBOOK ON FINANCIAL REGULATION 569 (Niamh Moloney et al. eds., 2015) (describing the "supranational" approach to regulating financial market infrastructures, with "international regulatory guidelines and principles adopted by the G20 . . . [and] developed by the Financial Stability Board" (footnote omitted)). The G20—or Group of Twenty—is composed of nineteen countries plus the European Union, and "is the premier forum for its members' international economic cooperation and decision-making." *About G20*, G20 2015 TURK., https://g20.org/about-g20/ (last visited Nov. 15, 2015). The Financial Stability Board (FSB) is "an international body that monitors and makes recommendations about the global financial system." *About the FSB*, FIN. STABILITY BD., http://www.financialstabilityboard.org/about/ (last visited Nov. 15, 2015). According to the Board's website:

> The FSB promotes international financial stability; it does so by coordinating national financial authorities and international standard-setting bodies as they work toward developing strong regulatory, supervisory and other financial sector policies. . . .
>
> The FSB, working through its members, seeks to strengthen financial systems and increase the stability of international financial markets. The policies developed in the pursuit of this agenda are implemented by jurisdictions and national authorities.

Id.

payments, securities, derivatives, or other financial transactions," which "include payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories."[70] These types of systems act as the networks, or the "plumbing systems," through which money and other forms of value flow in our modern economy.[71]

As the Federal Reserve notes, "Financial market infrastructures . . . are critical components of the nation's financial system . . . . The safety and efficiency of these systems may affect the safety and soundness of U.S. financial institutions, and in many cases, are vital to the financial stability of the United States."[72] In adopting standards for financial market infrastructures, the Federal Reserve's "objective is to foster the safety and efficiency of payment, clearing, settlement, and recording systems and to promote financial stability, more broadly."[73]

The consequences of failure in a system that serves as financial market infrastructure are severe, with "a failure [possibly] lead[ing] ultimately to a disruption in the financial markets more broadly and undermin[ing] public confidence in the nation's financial system."[74] Further, the interconnectedness and interdependence inherent among financial market infrastructures mean that they can function as "transmission channel[s] of systemic risk."[75] The 2008 financial crisis made everyone aware of just how easily risk can be transmitted through our financial system, and financial market infrastructures provide the pathways for that transmission.

Although the Federal Reserve policies described above note how critical financial market infrastructure is to the stability of the *U.S.* financial system, it is clear that they are also crucial to global financial stability, given the international character of our financial system today.[76] With the renewed emphasis on financial stability since the 2008 financial crisis, "governments and regulators of the leading economies" worked together to reach an "international consensus" on "key guiding principles" and "more detailed guidelines" to support the stability of financial market infrastructures,[77] with many countries basing their policies on the April 2012 *Principles for Financial Mar-*

70. Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. 67,326, 67,333 (Nov. 12, 2014).
71. *See id.*
72. *Id.*
73. *Id.*
74. *Id.* at 67,334.
75. *Id.*
76. *See* Ferrarini & Saguato, *supra* note 69, at 571.
77. *Id.*

ket Infrastructures (PFMI) report by the Committee on Payment and Settlement Systems (CPSS) and Technical Committee of the International Organization of Securities Commissions (IOSCO).[78]

The international guidelines for financial market infrastructures seek to mitigate risks to the structures to help maintain their stability. According to the Federal Reserve's Policy on Payment System Risk, "the basic risks in payment, clearing, settlement, and recording systems may include credit risk, liquidity risk, operational risk, and legal risk."[79] The international PFMI adds systemic risk, general business risk, and custody and investment risks to that list.[80] This Article focuses on *operational risk*, which the Federal Reserve defines as:

> the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the [financial market infrastructure] . . . . includ[ing] physical threats, such as natural disasters and terrorist attacks, and information security threats, such as cyberattacks. Further, deficiencies in information systems or internal processes include errors or delays in processing, system outages, insufficient capacity, fraud, data loss, and leakage.[81]

Global financial regulators have identified a number of principles to help financial market infrastructures lessen their risks. Particularly relevant to my analysis are those dealing with operational risks spawned by governance structures and technology. From the PFMI, these include:

> *Principle 2: Governance:* An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.
>
> . . . .
>
> *Principle 3: Framework for the comprehensive management of risks:* An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks.
>
> . . . .
>
> *Principle 17: Operational risk:* An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies,

78. *See* PFMI, *supra* note 17.
79. Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. at 67,334.
80. *See* PFMI, *supra* note 17, at 18–20.
81. Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. at 67,334 n.8.

> procedures, and controls. Systems should be designed to have a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.[82]

As I discuss in Part III below, these risk mitigation principles are problematic for Bitcoin and likely for other decentralized virtual currencies. In Part III, I lay out the operational risks of Bitcoin in relation to its blockchain's potential role as financial market infrastructure. As I will discuss, Bitcoin's most fundamental features generate important operational risks whose mitigation would require, in some cases, an abandonment of the core premises of the virtual currency. Most notably, the governance and risk management standards for financial market infrastructures seem impossible in a system premised on decentralization, which only exacerbates the technology risks involved.

Of course, it is currently inappropriate to categorize the Bitcoin blockchain as financial market infrastructure because of its limited use and the relatively small values that are moved across its network. Systems don't become "financial market infrastructure" in regulators' eyes until they reach a certain scale. For instance, the Federal Reserve's Policy on Payment System Risk applies only to payment systems of a certain scale—those that "expect to settle a daily aggregate gross value of U.S. dollar-denominated transactions exceeding $5 billion on any day during the next 12 months."[83] Obviously, the Bitcoin blockchain supports exchange values that are nowhere close to that size at the moment;[84] however, blockchain proponents are targeting replacing precisely the systems that comprise existing financial market infrastructures,[85] so a discussion of how regulators treat existing financial market infrastructures is worthwhile. It is clearly better to consider the operational risks generated by Bitcoin's fundamental structures *now* rather than waiting until we are widely *relying* on the Bitcoin blockchain as infrastructure, and *then* realizing that its fundamental structures make it unreliable. With that goal in mind, in the next Part, I describe key operational risks that undermine the Bitcoin blockchain's reliability as potential financial market infrastructure.

---

82. PFMI, supra note 17, at 1–3.

83. Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. at 67,335.

84. *See* Wild et al., *supra* note 61 ("On an average day more than 120,000 transactions are added to bitcoin's blockchain, representing about $75m exchanged.").

85. *See supra* notes 61–66 and accompanying text.

III.
Bitcoin's Operational Risks and Its Potential as Financial Market Infrastructure

Given that blockchain technology is being discussed as a potential disruptor of certain financial market infrastructures, the reliability of the technology is paramount. Therefore, in this Part, I explicate important risks to Bitcoin's operation—particularly focusing on the technology and governance risks that are generated by Bitcoin's most basic features.

These structural features are:

(1) its status as software;
(2) its decentralized structure;
(3) its open-source software development process; and
(4) its expertise problem.[86]

In the Sections that follow, I examine the operational risks created by each of these core features, and then discuss how these risks undermine the Bitcoin blockchain's reliability as financial market infrastructure.[87]

A. *Bitcoin as Software*

At its most basic level, Bitcoin is software, and living in a computer-driven, digital world has made all of us intimately familiar with

---

86. There are certainly other risks that threaten Bitcoin's ongoing operation. *See generally* Mariam Kiran & Mike Stannett, NEMODE, Bitcoin Risk Analysis (2014), http://www.nemode.ac.uk/wp-content/uploads/2015/02/2015-Bit-Coin-risk-analysis.pdf (considering, among other risks: technology risks including reliance of the Bitcoin system on the availability of high-powered mining computers only produced by a few companies worldwide, the possibility of malware affecting the Bitcoin code, miners taking advantage of software errors to increase their rewards, the vulnerability of miners to attacks, the concentration of miners making their exposure to natural disasters relevant to the network operating); Gareth W. Peters et al., Opening Discussion on Banking Sector Risk Exposures and Vulnerabilities from Virtual Currencies: An Operational Risk Perspective 20–23, 28–30 (2014), http://arxiv.org/pdf/1409.1451.pdf (examining how the operational risks of virtual currencies, including, among others, the risks of an organized attack on the system, transaction malleability, and double-spending, reliance on IT of mining network, and software problems, could impact the banking sector). In this Article, I focus on the risks I consider most urgent. I also do not mean to suggest that these risks are unfamiliar to regulators, academics, the media, or members of the Bitcoin community. I do believe that they are worth explicitly considering, though, in the context of the Bitcoin blockchain's function as potential financial market infrastructure.

87. I do not attempt to state the likelihood that a particular risk will lead to the Bitcoin network's collapse, although that would be a valuable area of further research. I consider each risk to have potentially catastrophic consequences for Bitcoin if it materializes. Thus, I am satisfied that even if the risk has a very low chance of coming to fruition, it should still be relevant in making decisions about Bitcoin.

the problems endemic to software. To list but a few that are readily perceived by non-techies like myself:

(1) software always has bugs;
(2) software is vulnerable to attack;
(3) software is ever-changing through new releases; and
(4) few people understand how software works.

In this Subpart, I discuss each of these weaknesses of software, and explain why that weakness is problematic for the Bitcoin blockchain's function as financial market infrastructure.

1. Software Always Has Bugs

According to computer experts, "software today remains, in many ways, far less reliable and more prone to bugs than in the past."[88] It is widely acknowledged that there is no such thing as flawless software; there are always errors or "bugs" that negatively affect the performance of the software or make it vulnerable to attacks by hackers.[89] This has been a problem since computers were created, and even with our amazing and rapid improvements in technology, software—like the humans who create it—remains inherently imperfect.[90]

Errors in software may be introduced in many different ways, including the programmer's lack of understanding or expertise in the programming language or the software structure or goals; the incompatibility of different releases of software; sloppiness, carelessness, or rushing on the part of the programmer; poorly coordinated collaboration; lack of big-picture oversight; miscommunications between programmers; and any other number of situations that cause people to create imperfect products.[91]

---

88. Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1022 (2014) (internal quotation marks omitted) (quoting Claire Le Goues et al., *The Case for Software Evolution*, 18 PROC. FSE/SDP WORKSHOP 205, 205 (2010)) (arguing for regulation tailored toward improving cyber-security through mitigation of harms rather than elimination of threat).

89. I discuss software's vulnerability to attacks in relation to Bitcoin in Part III.A.2, *infra*.

90. *See* Bambauer, *supra* note 88, at 1021 ("Software is . . . structurally prone to failure, despite significant efforts to remediate it. . . . Eliminating bugs completely is simply impossible.").

91. For a discussion of how people dynamics and skills are determinative of the quality of software, see generally ROBERT GLASS, FACTS AND FALLACIES ABOUT SOFTWARE ENGINEERING (2003).

As an example, the "catastrophic" Heartbleed bug that was discovered in OpenSSL in April 2014[92] came about through a coding error that a contributor to the open-source software "unfortunately . . . missed" when he submitted it to the core developers for the project.[93] The core developer who reviewed the suggested code to determine whether to accept it into the next release version of the software "apparently also didn't notice" the error, "so the error made its way from the development branch into the released version."[94] The developer who wrote the buggy code said the error was "quite trivial," but the impact was "severe."[95] Indeed, the impact was so severe that the U.S. Department of Homeland Security issued a public security alert about Heartbleed,[96] and a group of leading technology companies immediately created an initiative to jointly fund the development of open-source software that, like Open SSL, is a critical part of the Internet's security infrastructure.[97] This initiative was immediately put to work when the even more damaging Shellshock bug—lurking for twenty-two years—was discovered in September 2014 in Bash software, an-

---

92. Open SSL is open-source software that provides part of the fundamental security structure of the Internet, and the Heartbleed bug made available to hackers private information, such as passwords, credit card data, and other personal information from supposedly secure transactions. Computer security experts deemed it "catastrophic." *See* Brian X. Chen, *Q. and A. on Heartbleed: A Flaw Missed by the Masses*, N.Y. TIMES: BITS (Apr. 9, 2014, 2:26 PM), http://bits.blogs.nytimes.com/2014/04/09/qa-on-heartbleed-a-flaw-missed-by-the-masses/.

93. Ben Grubb, *Man Who Introduced Serious 'Heartbleed' Security Flaw Denies He Inserted It Deliberately*, SYDNEY MORNING HERALD (Apr. 11, 2014), http://www.smh.com.au/it-pro/security-it/man-who-introduced-serious-heartbleed-security-flaw-denies-he-inserted-it-deliberately-20140410-zqtal.html (quoting Robin Seggelmann, author of the code containing the Heartbleed bug).

94. *Id.*

95. *Id.*

96. *See, e.g.*, Larry Zelvin, Dir. of the Nat'l Cybersec. & Commc'ns Integration Ctr., *Reaction on "Heartbleed": Working Together to Mitigate Cybersecurity Vulnerabilities*, DEP'T HOMELAND SEC. BLOG (Apr. 11, 2014, 7:52 AM), http://www.dhs.gov/blog/2014/04/11/reaction-%E2%80%9Cheartbleed%E2%80%9D-working-together-mitigate-cybersecurity-vulnerabilities-0 (providing information on Heartbleed, the government's response, and steps for the public to take to protect itself).

97. *The Linux Foundation's Core Infrastructure Initiative Announces New Backers, First Projects to Receive Support and Advisory Board Members*, LINUX FOUND. (May 29, 2014, 4:56 AM), http://www.linuxfoundation.org/news-media/announcements/2014/05/core-infrastructure-initiative-announces-new-backers (describing the private initiative, funded by large companies including Facebook, Google, HP, and others, to fund development of open-source software that "support[s] critical infrastructure"); *see also* Nicole Perlroth, *A Contradiction at the Heart of the Web*, N.Y. TIMES, Apr. 19, 2014, at B1 (discussing how the underfunding of Open SSL software development contributed to developers creating and failing to identify the Heartbleed bug).

other open-source project that forms a key part of the Internet infrastructure.[98]

Unsurprisingly, the Bitcoin code is known to have errors that cause glitches in its operations.[99] The Bitcoin software development website includes a list of bugs that have already been identified and need fixes,[100] and there are instructions for software developers to send encrypted descriptions of critical bugs they discover to the Bitcoin core developers.[101] As the list of known bugs implies, the core software is always being rewritten to resolve these issues. Further, a 2014 study performed by a Bitcoin advocacy organization entitled *Removing Impediments to Bitcoin's Success: A Risk Management Study* (the "Risk Management Study") identified the existence of a significant bug in either the Bitcoin protocol or code as a "low-likelihood, high consequence threat" to Bitcoin (although it concluded that continued operation of the code is the most appropriate way to discover and remedy any existing bugs).[102] Finally, even the primary core de-

98. *See* Perlroth, *supra* note 97, at B1 (reporting on Shellshock, a "particularly alarming software bug that could be used to take control of hundreds of millions of machines around the world, potentially including Macintosh computers and smartphones that use the Android operating system" that was discovered in Bash, "a free piece of [open-source] software that is now built into more than 70 percent of the machines that connect to the Internet").

99. *See Issues List*, GITHUB, https://github.com/bitcoin/bitcoin/labels/Bug (last visited Oct. 22, 2015) (showing that in the Bitcoin software development repository, there are 79 unresolved bugs while 427 reported bugs have been resolved); *see also* Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP. 213, 228 (2015), http://ssrn.com/abstract=2495572 ("[T]he Bitcoin platform faces operational risks through potential vulnerabilities in the protocol design . . . ."); Vasilis Kostakis & Chris Giotitsas, *The (A)Political Economy of Bitcoin*, TRIPLEC: COMMC'N CAPITALISM & CRITIQUE (2014), http://www.triple-c.at/index.php/tripleC/article/view/606/578 (noting that "[b]eing still in development it is yet unknown how many bugs are hidden in the [Bitcoin] code").

100. *Issues List*, *supra* note 99.

101. The instructions provide:

> If you find a vulnerability related to Bitcoin, non-critical vulnerabilities can be emailed in English to any of the core developers or sent to the private bitcoin-security mailing list listed above. An example of a non-critical vulnerability would be an expensive-to-carry-out denial of service attack. Critical vulnerabilities that are too sensitive for unencrypted email should be sent to one or more of the core developers, encrypted with their PGP key(s).

Contribute Bug Reports, BITCOIN, https://bitcoin.org/en/bitcoin-core/contribute/issues (last visited Oct. 6, 2015).

102. BITCOIN FOUND., REMOVING IMPEDIMENTS TO BITCOIN'S SUCCESS: A RISK MANAGEMENT STUDY 20–21 (2014), https://bitcoinfoundation.org/wp-content/uploads/2014/07/Bitcoin-Risk-Management-Study-Spring-2014.pdf [hereinafter RISK MANAGEMENT STUDY].

veloper for Bitcoin has acknowledged his fears of an undiscovered catastrophic bug lurking in the code.[103]

Why This Is a Problem for Bitcoin as Financial Market Infrastructure

Technology risk is not new to our financial market infrastructures, as they already rely on software to operate in most cases. So, Bitcoin may be no riskier than other financial market infrastructures in this regard. A valuable avenue for further research would be some specific empirical comparisons between the software for particular financial market infrastructures and Bitcoin.

It is important not to assume, though, that just because Bitcoin is newer, it is necessarily less buggy. It is even more important to consider how Bitcoin's governance structures, or lack thereof, help to magnify its technology risks, as I discuss in Sections III.B and III.C below.

2. *Software Is Vulnerable to Attack*

As we all know, hacking is already an omnipresent threat to modern software and is only increasing. There are daily reports of significant and damaging security breaches and data thefts that result from computer hackers exploiting errors in software.[104] Although there are ongoing efforts to resist hacking, it is a rare person who will argue that any software is completely invulnerable to hacking. As the Financial Security Oversight Council noted in its 2015 annual report, "recent cyber attacks have heightened concerns about the potential of an even more destructive incident that could significantly disrupt the workings of the financial system."[105]

Thus, the security of the Bitcoin software and network are of fundamental importance in evaluating the Bitcoin blockchain as potential

103. *See* Simonite, *supra* note 37.

104. *See, e.g.*, Brian X. Chen, *Apple Says It Will Add New iCloud Security Measures After Celebrity Hack*, N.Y. Times: Bits (Sept. 4, 2014, 11:32 PM), http://bits.blogs.nytimes.com/2014/09/04/apple-says-it-will-add-new-security-measures-after-celebrity-hack/ ("Apple said on Thursday that it would strengthen its security measures after a recent episode where hackers broke into the Apple accounts of a number of celebrities, stole their nude photos and leaked them on the Internet."); David E. Sanger & Nicole Perlroth, *Bank Hackers Steal Millions via Malware*, N.Y. Times, Feb. 15, 2015, at A1 (reporting the February 2015 discovery that "more than 100 banks and other financial institutions in 30 nations" were robbed by a team of hackers in what may be "one of the largest bank thefts ever"); Robin Sidel, *Home Depot's 56 Million Card Breach Bigger than Target's*, Wall St. J. (Sept. 18, 2014, 5:43 PM), http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571 (describing the security breaches at Home Depot, Target, and other merchants).

105. Fin. Stability Oversight Council, *supra* note 62, at 3.

financial market infrastructure. It is important here to distinguish between (a) vulnerabilities of the Bitcoin software and network and (b) vulnerabilities of companies that service those who participate in the Bitcoin network. The Bitcoin ecosystem now contains numerous intermediaries, such as exchanges, wallet companies, and payment processors, which hold bitcoins as part of their business models.[106] Many of these intermediaries have been hacked in attempts to steal the bitcoins they hold.[107] Importantly, though, attacks on intermediaries in the Bitcoin ecosystem are not attacks on the Bitcoin software and network itself. While an attack on an intermediary (such as an individual exchange) only affects the particular bitcoins being handled or held by that exchange,[108] an attack on the Bitcoin software or network could have the much more severe consequence of simultaneously halting the exchange of *all* bitcoins. Attacks on the Bitcoin software or network are therefore a systemic operational risk to the Bitcoin blockchain as financial market infrastructure.

Bitcoin proponents argue that the Bitcoin software and network have extremely strong security features that make it difficult if not impossible for Bitcoin to be attacked.[109] For instance, the decentralized structure of the network makes it impossible to ensure that all nodes within the Bitcoin network could necessarily be reached simultaneously in an attack (unless, of course, one of the core developers

---

106. Examples of Bitcoin exchanges include Coinbase, BitStamp, ItBit, and OKCoin. Examples of Bitcoin wallet companies include Circle, Armory, DarkWallet, and Blockchain. Examples of Bitcoin payment processors include BitPay and Coin.co.

107. *See, e.g.*, Richard Boase, *Hackers Steal $1.2 Million of Bitcoins from Inputs.io, a Supposedly Secure Wallet Service*, CoinDesk (Nov. 7, 2013), http://www.coindesk.com/hackers-steal-bitcoins-inputs-io-wallet-service/ (reporting on theft of bitcoins from wallet service); Stan Higgins, *BTER Claims $1.75 Million in Bitcoin Stolen in Cold Wallet Hack*, CoinDesk (Feb. 15, 2015), http://www.coindesk.com/bter-bitcoin-stolen-cold-wallet-hack/ (reporting on the alleged hack of China Bitcoin exchange BTER, with $1.75 million in bitcoins stolen); Ahmed Murad, *Hackers Breach Bitcoin Exchange*, Fin. Times, Jan. 7, 2015, at 13 (reporting on hack of U.K. Bitcoin exchange BitStamp, with the theft of 19,000 bitcoins worth about $5 million).

108. Of course, an attack on a major exchange or other significant actor in the Bitcoin ecosystem could affect the value of all bitcoins by causing the public to lose faith in Bitcoin, as was the case when Mt. Gox reported losing $450 million worth of bitcoins during its collapse in February 2014. *See* Murad, *supra* note 107. A leading Bitcoin price index showed that the price of a bitcoin fell from around $800 on February 6, 2014 to around $700 on February 7, 2014 as Mt. Gox paused withdrawals prior to its collapse. *See Bitcoin Price Index Chart*, CoinDesk, http://www.coindesk.com/price/ (last visited Oct. 25, 2015).

109. *See, e.g.*, Antonopoulos, *supra* note 23, at 211, 213; Campbell R. Harvey, Bitcoin Myths and Facts 5 (Aug. 18, 2014) (unpublished manuscript), http://ssrn.com/abstract=2479670 ("Bitcoin is probably the most secure form of transaction in the history of the world. . . . [T]o break into the blockchain, you would need an enormous amount of computing power.").

were forced by an attacker to send an emergency message to all nodes that allowed a network-wide attack through the adoption of malicious code).[110] Further, proponents explain that it is extremely difficult if not impossible to tamper with the blockchain and that older parts of the blockchain (those reflecting Bitcoin transactions that occurred in the past) become more and more immutable and robust over time.[111]

Yet, there are widely acknowledged vulnerabilities to which Bitcoin is susceptible that malicious actors could exploit to disrupt Bitcoin's operation. The most prominent threat is known as the "51% Attack."[112] This type of attack would come from parties who control at least 51% of the computing power[113] that the Bitcoin system uses to validate transactions and create the blockchain (or transaction ledger).[114] Although this type of attack was largely theoretical in the early days of Bitcoin because the miners who validated Bitcoin transactions were mostly individuals, it is possible today given the growth of large "mining pools" that control significant portions of the Bitcoin computing power (and hence, have enough "votes" to control which transactions are validated and what shows up on the blockchain).[115]

The effects of such an attack could be to revise recently settled transactions on the blockchain and to prevent current and future transactions from being completed.[116] Given that Bitcoin's primary benefit is the reliability of the blockchain, any ability to tamper with it or to

---

110. *See* ANTONOPOULOS, *supra* note 23, at 157, 211.

111. *See id.* at 211; Harvey, *supra* note 109, at 5. *But see* Simon Barber et al., *Bitter to Better: How to Make Bitcoin a Better Currency*, *in* 16 INT'L CONF. ON FIN. CRYPTOGRAPHY & DATA SECURITY 399, 404–06 (2012). In this computer science paper, the authors describe the increasing and "very real" risk of a "history-revision" attack that could rewrite the Bitcoin blockchain, replacing real transactions with made-up ones. The authors propose solving this problem by automating the creation of authoritative copies of the blockchain, creating "checkpoints." Barber et al., *supra*, at 404–06. The authors note that the Bitcoin core developers already do create "checkpoints" of the blockchain that they push out with new software releases, but argue that putting the creation of checkpoints in the hands of the developers makes them unreliable. *Id.*

112. *See, e.g.*, ANTONOPOULOS, *supra* note 23, at 211; JOSHUA A. KROLL ET AL., THE ECONOMICS OF BITCOIN MINING, OR BITCOIN IN THE PRESENCE OF ADVERSARIES 11–12 (2013), http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf; Barber et al., *supra* note 111.

113. Such an attack on the blockchain could succeed even with less than a 51% share of the computing power, with claims that as little as 30% of the computing power could succeed in this type of attack. *See* ANTONOPOULOS, *supra* note 23, at 212; Ittay Eyal & Emin Gun Sirer, *Majority Is Not Enough: Bitcoin Mining Is Vulnerable* (demonstrating, in a controversial computer science paper, that "selfish miners" of any portion of ownership could collude to control the Bitcoin network), *in* 18 INT'L CONF. ON FIN. CRYPTOGRAPHY & DATA SECURITY 436 (2014).

114. *See* ANTONOPOULOS, *supra* note 23, at 211–12.

115. *Id.*

116. *Id.*

manipulate its creation is highly damaging to the reliability of the system, and therefore to its credibility as financial market infrastructure. The attacker could also "double-spend" its own previously spent bitcoins—in effect, committing theft.[117]

While theft could be one motivation for orchestrating such an attack, another motivation could simply be to bring down Bitcoin, particularly if it becomes more widely used.[118] To obtain the requisite computing power would require "enormous investment," but such an attack "could conceivably be launched by a well-funded, most likely state-sponsored, attacker."[119]

Bitcoin proponents have argued that a 51% attack is highly unlikely for several reasons. First, the attack would be extremely expensive to conduct because obtaining the needed computing power would cost so much.[120] Second, after spending all the money to accumulate all the computing power, it would be against the attacker's financial interest to destroy the system in which it had invested so much.[121] And third, the 51% threshold has already been hit by certain mining pools, and they have not yet performed such an attack.[122]

Unfortunately, none of these reasons provide comfort that a 51% attack is impossible. Certain individuals and industries with great wealth could decide that it was in their interest to invest enough to destroy the credibility of Bitcoin. For instance, there has been much public discussion about how Bitcoin and other virtual currencies threaten the current model of financial services,[123] a trillion-dollar in-

117. *Id.*

118. *Id.* at 212–13.

119. *Id.* at 213.

120. *Id.*; Harvey, *supra* note 109, at 5–6.

121. *See* KROLL ET AL., *supra* note 112, at 12–13 ("[A] 51% . . . attack [by a mining cartel] is unlikely to generate enough reward within the Bitcoin economy to be worthwhile to the attacker."); *see also* Daniel Cawrey, *Are 51% Attacks a Real Threat to Bitcoin?*, COINDESK (June 20, 2014), http://www.coindesk.com/51-attacks-real-threat-bitcoin/ (stating that miners, "whose profits depend largely on the price of bitcoin being high . . . [have] no real incentive to attack the network").

122. *See* Jon Matonis, Exec. Dir. of the Bitcoin Found., *The Bitcoin Mining Arms Race: GHash.io and the 51% Issue*, COINDESK (July 17, 2014), http://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue/ (arguing that tensions have eased about the threat of a mining pool executing a 51% attack after a July 9, 2014 meeting of miners in London resulted in the GHash.io mining pool pledging to "do all it can to limit its share of the total bitcoin network to 39.99%").

123. *See* Aaron Timms, *Big Banks Are Confident in the Face of the Bitcoin Threat*, INSTITUTIONAL INV. (Oct. 10, 2014), http://www.institutionalinvestor.com/inside-edge/3389462/Big-Banks-Are-Confident-in-the-Face-of-the-Bitcoin-Threat.html#.VQSCj47F8nU (discussing the banking industry's response to claims that Bitcoin could "unbundle the banks" and "reimplement the entire financial system as a distributed system as opposed to a centralized system"). This threat may have changed now

dustry.[124] States could also decide that it was in their best interest to destroy Bitcoin and be willing to devote enough resources to complete such an attack.[125] If Bitcoin became more widely used, or if its blockchain began to serve as the backbone of significant financial infrastructures, there would be plenty of states (e.g., North Korea) or terrorist actors (e.g., ISIS) who would have both the incentives and resources to attempt this type of attack. Moreover, the fact that those parties who have held the relevant threshold of computing power have not used it to harm Bitcoin in the past, does not mean that this will always be the case. Finally, the more widely known and used Bitcoin becomes and the greater a role it plays as financial market infrastructure, the more attractive a target it becomes for those with an interest in destroying it.

While the 51% attack is the most widely acknowledged threat to Bitcoin's operation, distributed denial of service (DDOS) attacks could also disrupt the operation of the Bitcoin network, and therefore its blockchain. For example, in early March 2015, there was a wave of DDOS attacks against at least five Bitcoin mining pools, including one of the larger pools, GHash.Io.[126] With GHash.Io, the attack resulted in the pool being unable to mine bitcoins for hours at a time.[127] DDOS attacks against miners in the Bitcoin network have been a recurrent problem since 2011.[128] Given that the mining process is actually the

---

that the financial industry seems to be embracing blockchain technology as a whole, so may no longer have an incentive to destroy Bitcoin. However, destroying Bitcoin could demonstrate that the permissioned blockchains being developed by the financial industry are superior to Bitcoin and allow the financial industry to maintain control over financial market infrastructures.

124. *See The Financial Services Industry in the United States*, U.S. DEP'T COM., http://selectusa.commerce.gov/industry-snapshots/financial-services-industry-united-states (last visited Mar. 8, 2015) ("In 2012, finance and insurance represented 7.9 percent (or $1.24 trillion) of U.S. gross domestic product.").

125. *See* KROLL ET AL., *supra* note 112, at 13 (arguing that "governments are the most plausible source" of a 51% attack on Bitcoin from outside the Bitcoin network).

126. *See* Stan Higgins, *Bitcoin Mining Pools Targeted in Wave Of DDOS Attacks*, COINDESK (Mar. 12, 2015), http://www.coindesk.com/bitcoin-mining-pools-ddos-attacks/ (reporting that mining pools AntPool, BW.com, NiceHash, CKPool, and GHash.io were hit by DDOS attacks, with hackers demanding ransoms to end the attack).

127. *See* Julia McGovern, *Official Statement on the Last Week's DDoS-Attack Against GHash.IO Mining Pool*, CEX.IO BLOG (Mar. 16, 2015), http://blog.cex.io/news/official-statement-on-the-ddos-attack-against-ghash-io-mining-pool-13355 (reporting on the GHash.IO mining pool on a DDoS attack it suffered the week of March 7, 2015 that prevented miners from mining for six hours, with the hacker demanding five to ten bitcoins to end the attack).

128. *See* Benjamin Johnson et al., *Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools*, 2014 FIN. CRYPTOGRAPHY WORKSHOPS 72, 73 (evaluating the incentives that miners have to inflict DDOS attacks on one another); Marie

process that verifies bitcoin transactions and makes additions to the shared ledger, a simultaneous attack against many or all miners could compromise the Bitcoin network. As the Bitcoin mining industry continues to consolidate,[129] this threat becomes greater, as there are fewer targets that hackers must hit to achieve a network-wide outage.

Additional vulnerabilities of the Bitcoin software and protocol could emerge through improvements in mathematical cryptanalysis or through quantum computing.[130] This means that the cryptography that underlies Bitcoin could become less impenetrable (and thus more vulnerable) due to advances in our knowledge of mathematics, or that the computers that work to solve the algorithms in Bitcoin could become so much more powerful that the algorithms can be too easily solved.

There is also the problem identified by Donald Rumsfeld in regards to weapons of mass destruction in Iraq that applies to all forms of risk assessment:

> [A]s we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.[131]

There is simply no way to identify Bitcoin's "unknown unknowns"—the flaws that parties might be able to exploit (to their benefit and/or Bitcoin's detriment) in the future. The devastating Heartbleed bug, hidden in plain sight in the OpenSSL code, is a reminder of how software vulnerabilities can lurk undetected, a risk of which Bitcoin's own core developers are well aware.[132]

Vasek et al., *Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem*, 2014 Fin. Cryptography Workshops 57, 68 (estimating 142 DDOS attacks on the Bitcoin ecosystem between May 2011 and October 2013, with 38% of those attacks on mining pools, and noting that "over 60% of large mining pools have been DDoSed, compared to just 17% of small ones").

129. *See* Nermin Hajdarbegovic, *Acquisitions and Partnerships Fuel Bitcoin Mining Sector Expansion*, CoinDesk (Aug. 25, 2014), http://www.coindesk.com/acquisitions-partnerships-fuel-bitcoin-mining-sector-expansion/ (reporting on recent, rapid consolidation in the Bitcoin mining industry).

130. Email from Shawn Bayern, Larry & Joyce Beltz Professor of Torts at Fla. State Univ. Coll. of Law, to author (Jan. 20, 2015, 11:33 PM) (on file with author); *see also* Böhme et al., *supra* note 99, at 228 ("[T]he Bitcoin platform faces systemic operational risks through . . . breakthroughs in cryptanalysis.").

131. Donald H. Rumsfeld, U.S. Sec'y of Def., News Briefing (Feb. 12, 2002), http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

132. *See* Simonite, *supra* note 37.

Why This Is a Problem for Bitcoin as Financial Market Infrastructure

Clearly, Bitcoin shares its vulnerability to hacking with existing digital financial market infrastructure, so perhaps does not pose a *greater* technology failure risk than they do, and may even be more resilient. However, though many have suggested it is highly resistant to hacking, it is important to remember that it is not *invulnerable*.

Bitcoin's susceptibility to a 51% attack creates a new type of technology risk, however, which appears difficult to overcome with its existing design. As noted above, if the Bitcoin blockchain were to become more widely used, perhaps as the architecture of a large payment system, it would be an extremely tempting target for an attack by a terrorist group, as its failure would be a devastating event to all who rely on that infrastructure. Indeed, the recent cyberattack on Sony Corporation—possibly by North Korea[133]—should give us pause in creating such a high-consequence target that determined attackers could bring down. While it is true that the Bitcoin system is small now, if more of our financial systems begin to rely on it, this risk will become more significant.

3. Software Is Ever-Changing Through New Releases

Software is always on the move. Rather than being a static creation, during the period that software remains in use, it is generally changing as different versions or "releases" of the software are issued by software developers. New versions of software are created to fix bugs or to introduce new features and may be incompatible with earlier versions of the software. For example, the release notes for the tenth version of the Bitcoin software, released by the core developers in February 2015, state that it is incompatible with prior versions of the software.[134]

New versions of the Bitcoin code have already caused serious problems for the Bitcoin network. There has been uneven updating to newer versions of software by the computers that operate the Bitcoin

133. *See* David E. Sanger & Martin Fackler, *Tracking the Cyberattack on Sony to North Koreans*, N.Y. TIMES (Jan. 19, 2015), http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html (reporting on President Obama's statement that North Korea was responsible for the November through December 2014 cyberattack on Sony Pictures and that the United States would retaliate).

134. *See* Wong, *supra* note 35; *Upgrading and Downgrading: Downgrading Warning*, GITHUB, https://github.com/bitcoin/bitcoin/blob/0.10/doc/release-notes.md (last visited Mar. 13, 2015) (stating that "the block files and databases are not backwards-compatible with pre-0.10 versions of Bitcoin Core or other software").

network (the "nodes" and "miners"), and this has resulted in potentially catastrophic consequences.

For instance, in March 2013, Bitcoin experienced a "hard fork" in the software, meaning that two separate blockchains (or transaction histories) were being simultaneously developed by computers within the Bitcoin network.[135] The fork was "due to nodes using two different versions of the bitcoin protocol"[136] and meant that there were effectively two ledgers being kept for Bitcoin transactions. This throws the entire system into chaos because Bitcoin's core principle is that the common ledger is reliable and true. Although the network recovered from this fork through the collaboration of the core software developers and certain mining pools (as discussed in Section III.B), this demonstrates the system-wide risks posed by uneven updating of new releases of software.

Perhaps even more significant is the epic struggle between versions of the Bitcoin core software that is ongoing as of this writing. Referred to as the "block size debate," this dispute amongst the Bitcoin core (and other) developers deals with how much computer memory the files within the blockchain should consume.[137] Viewed as a matter that must be addressed in order for Bitcoin to operate smoothly on a larger scale (i.e., to accommodate more changes to the blockchain as would need to be the case if other financial market infrastructures utilized it), the matter has come to a head, with various versions of the Bitcoin code proposed by different factions of developers.[138] For Bitcoin, adopting a new software release also means agreeing to the policy choices embedded in the code, and this dispute threatens to split the network—which could ultimately lead to separate "forked" blockchains.[139] As will be discussed in Sections III.B and III.C, new releases cannot be forced on anyone in the network, and

---

135. *See 11/12 March 2013 Chain Fork Information*, BITCOIN (Mar. 11, 2013) https://bitcoin.org/en/alert/2013-03-11-chain-fork.

136. FRANÇOIS R. VELDE, FED. RES. BANK CHI., BITCOIN: A PRIMER 3 (2013), https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317.

137. *See* Grace Caffyn, *What Is the Bitcoin Block Size Debate and Why Does It Matter?*, COINDESK (Aug. 21, 2015), http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/.

138. *See id.*

139. *See* Arvind Narayanan & Andrew Miller, *Bitcoin Faces a Crossroads, Needs an Effective Decision-Making Process*, FREEDOM TO TINKER (May 11, 2015), https://freedom-to-tinker.com/blog/randomwalker/bitcoin-faces-a-crossroads-needs-an-effective-decision-making-process/ (noting that the proposed versions of the Bitcoin software to address the block size problem reflect policy choices and affect different Bitcoin users differently).

they require adoption by a majority of the computing power in the network to take effect.[140]

Why This Is a Problem for Bitcoin as Financial Market Infrastructure

The evolving nature of software through new releases may be a bigger problem for decentralized Bitcoin than it is for more centralized financial market infrastructures. Since controversial new releases of Bitcoin software may be unevenly adopted, there would seem to be potential for periodic forks in the network when consensus cannot be found amidst the parties in the network. This undermines the reliability of the Bitcoin blockchain, as has already been demonstrated in the March 2013 fork. In a centralized financial market infrastructure, however, or even in "permissioned blockchains," new releases of software can likely be implemented more easily, since adopting the new version can be mandated on participants, perhaps through the contract that allows participation in the permissioned blockchain.

4. Few People Understand How Software Works

The final operational risk associated with Bitcoin's status as software that I will discuss is the fact that, as with all software, only a small percentage of the population understands how software works. Software coders have a particular expertise that makes the quality of their code, and even the basic functions it performs, opaque to people who are not experts in the relevant software language. The recent admission by Volkswagen that its software made the emissions of its vehicles appear lower than they actually were demonstrates clearly the power of software coders and the inability of non-coders to perceive problems or even illegal actions enabled by the code.[141] Software coding is truly an area in which knowledge (of code) is power.

Why This Is a Problem for Bitcoin as Financial Market Infrastructure

It is true that most people do not understand how existing financial market infrastructures work, any more than they understand how software works. Perhaps we already have an overly complex system that either no one or only a very select group of experts understands, and there is no way that virtual currencies make an already bad situation worse.

---

140. *See id.*

141. *See* Jim Dwyer, *Volkswagen's Diesel Fraud Makes Critic of Secret Code a Prophet*, N.Y. TIMES (Sept. 22, 2015), http://www.nytimes.com/2015/09/23/nyregion/volkswagens-diesel-fraud-makes-critic-of-secret-code-a-prophet.html (describing the dangers of secret software code and arguing that it should be inspected).

Yet, for the moment at least, virtual currency's complexity and the software and network knowledge required to truly understand it means that there is an even more limited number of people who understand it (assuming that anyone actually does).[142] This is because having a sophisticated understanding of Bitcoin or other virtual currencies requires extensive knowledge in multiple fields, likely including software coding, networks, cybersecurity, economics, payment systems, money, financial and economic history, finance, and surely many more. This is not to say that there aren't some amazing people who have mastered this array of fields, but that it is surely a very select group.

The fact that only a very limited portion of the population truly understands how Bitcoin operates gives rise to systemic operational risks. This is because it requires the population to put extreme amounts of trust in the skill and integrity of the people making decisions about the Bitcoin code and network. The larger the system becomes, with more "blockchain" companies using the Bitcoin network to accomplish their tasks,[143] the more pressure that is put on this small group of experts to make desirable policy choices[144] that they implement accurately and safely into the code. We should proceed with caution in building complex, opaque systems that carry out tasks of significant systemic importance.[145]

Something so difficult for non-experts to understand is difficult for regulators to address, as the world learned to its chagrin with the opaque credit-default swaps, shadow banking practices, and mortgage-backed securities that led us into the 2008 financial crisis.[146] Letting

142. *Cf.* Lo & Wang, *supra* note 58, at 7 (noting that "anecdotally, the typical [Bitcoin] user tends to be well versed in internet applications and even programming"); 2012 ECB Paper, *supra* note 38, at 27 (noting the complexity of Bitcoin and the "high-risk situation" created by the fact that users of it may not understand how it works).

143. *See* Shin, *supra* note 52.

144. Of course, the desirability of a particular policy choice for Bitcoin (Should there be transaction fees? Should the limit on total bitcoins be increased? What should the block size be?) will vary depending on which constituency is being asked.

145. The open-source nature of the Bitcoin code does mitigate this risk, as it allows other coders to evaluate the code. This contrasts with the proprietary nature of the Volkswagen code, which was unavailable to regulators or the public for scrutiny. *See* Dwyer, *supra* note 141. However, there is still a barrier between the expertise of the coders and the expertise of financiers and regulators—bridging the knowledge and communications gap between these groups is difficult and can lead to unexpected risks.

146. For a treatment of how the reliance on complicated financial structures and algorithms helped to create the 2008 financial crisis, see Scott Patterson, The Quants: How a New Breed of Math Whizzes Conquered Wall Street and Nearly Destroyed It (2010).

subject matter experts (in the case of finance, the "quants,"[147] and in the case of Bitcoin, the software developers) tell regulators "trust us, it works" is highly problematic from a risk-management perspective, particularly when we are talking about potential financial market infrastructure, and when more and more influential people and businesses are pushing virtual currencies forward and proclaiming them likely to be as transformative as the Internet.[148]

As demonstrated in this Part, the inescapable involvement of software in the ongoing operation and maintenance of the Bitcoin blockchain creates significant operational risks that must be considered if Bitcoin functions as financial market infrastructure.

B. Bitcoin's Decentralized Structure

Bitcoin is described almost universally as a "decentralized peer-to-peer" currency. This means that Bitcoin does not operate from a single server or central computer, but instead, "means, practically speaking, that the entire system is made up of versions of the software that end-users download and run on their personal computers."[149] This structure echoes other well-known peer-to-peer software programs such as BitTorrent or Grokster. Indeed Bitcoin's decentralization is described by the Bitcoin Foundation as "[a] key characteristic of Bitcoin and a source of its strength."[150]

Bitcoin's decentralized structure means that "there is a meaningful sense in which nobody is in charge of Bitcoin."[151] Bitcoin does not

---

147. *Id.*

148. *See, e.g.*, Andreessen, *supra* note 65 (comparing Bitcoin to the Internet in terms of its revolutionary potential); Tom Braithwaite & Ben McLannahan, *Master Joins Cryptocurrency Start-Up*, FIN. TIMES (Mar. 10, 2015), http://www.ft.com/cms/s/0/e29808a8-c744-11e4-9e34-00144feab7de.html#axzz3nQl8hY6t (reporting that Blythe Masters, who formerly was "instrumental in developing the credit default swaps market [at J.P. Morgan]" in the 1990s, had become CEO of Digital Asset Holdings, a trading platform for "big banks and asset managers" built on the Bitcoin blockchain); Kristin Broughton, *Former SEC Chairman Levitt to Advise Bitcoin Firms*, 179 AM. BANKER 167 (Oct. 29, 2014) (reporting that former SEC Chairman Arthur Levitt is advising Bitcoin companies BitPay and Vaurum); Matthew Heller, *Veteran Bank Exec Joins Bitcoin Startup as CFO*, CFO, http://ww2.cfo.com/people/2014/12/veteran-bank-exec-joins-bitcoin-startup-cfo/ (Dec. 12, 2014) (reporting that Paul Camp, "former head of JP Morgan Chase's global transaction services business, has become the latest executive to migrate from traditional banking and finance to the digital currency industry, joining startup Circle Internet Financial as CFO").

149. Bayern, *supra* note 33, at 1488.

150. RISK MANAGEMENT STUDY, *supra* note 102, at 2.

151. Bayern, *supra* note 33, at 1489. *But see* GERVAIS ET AL., *supra* note 36, at 54 (concluding that due to centralized mining and software development, "Bitcoin isn't a truly decentralized system as it is deployed and implemented today"); KROLL ET AL., *supra* note 112, at 18 (noting that "the lead developers of the open source [Bitcoin]

have an official organization or party that operates it. Instead, there is a sort of "unofficial" group of core software developers who maintain the code, including implementing fixes to flaws and introducing new features.[152] However, there is no single legal entity for which this group of software developers works in performing their maintenance of the Bitcoin software code, and these developers have no official responsibility to Bitcoin to perform their work to a certain standard or even to continue their work at all.

This setup creates a systemic operational risk for Bitcoin, as Bitcoin's ongoing operation is threatened by the fact that:

(1) there is no entity or person that assumes responsibility for the performance of Bitcoin;

(2) no one is in charge;

(3) it is impossible to tell who the voice of the group is; and

(4) there is no defined group that comprises Bitcoin or its management—just an amorphous, ever-shifting cluster of people who come and go within the group as they please.

Because of this decentralized structure, there is *no one* who is responsible for keeping the Bitcoin software operational. This means that even if there is a crucial repair that is needed to prevent complete collapse of the software, no one in particular would be *required* to perform the repair. Since no one is "responsible" for the code, even those core developers who have been voluntarily working to maintain Bitcoin may decide not to help in a moment of crisis, perhaps deeming their continued involvement to be personally risky.[153] It is true that in

---

software have become a de facto rules governance body for the Bitcoin economy"); BEN LAURIE, DECENTRALISED CURRENCIES ARE PROBABLY IMPOSSIBLE (BUT LET'S AT LEAST MAKE THEM EFFICIENT) 4 (2011), http://www.links.org/files/decentralised-currencies.pdf ("If Bitcoin is, indeed, using a known consensus group, then it has, after all, a central authority (that consensus group), and is not, therefore, a decentralised currency."); Grinberg, *supra* note 39, at 175 n.71 ("This development team constitutes the de facto central bank of Bitcoin.").

152. Bayern, *supra* note 33, at 1491 (noting that "Bitcoin does not operate in as rigorously decentralized a manner as Nakamoto originally designed it" and that "the developers of the Bitcoin client have the ongoing capacity to change the Bitcoin protocol in minor but incompatible ways, actively managing the community of Bitcoin users to make sure that the Bitcoin network upgrades in ways they have determined"); *see also* Danny Bradbury, *Why Bitcoin's Core Developers Want Multiple Versions*, COINDESK (Oct. 19, 2014), http://www.coindesk.com/bitcoins-core-developers-want-multiple-versions/ (describing the exclusive powers that the core developers have to make changes to the Bitcoin code).

153. Of course, analogous to employees and their stock options, coders who own substantial numbers of bitcoins have a financial incentive to keep the code operational in order to preserve their own wealth. Whether this is a sufficient incentive is an open question. I am grateful to Andrew Stephens for this insight.

prior moments of crisis, such as the March 2013 blockchain fork discussed below, the Bitcoin core developers worked to resolve the crisis,[154] but that does not prove that they may necessarily be relied upon to do so in the future.

In addition, decision-making may be slower than it needs to be to resolve an operational crisis, due to the fact that no one is in charge of Bitcoin. As there is no defined power or accountability structure, no one has to listen to anyone else's ideas about how to resolve a crisis. There are no definitively appointed decision-makers. This is different than having no one at all responsible for keeping the software operational; this risk is that even if people decide to take on responsibility for resolving a problem with the Bitcoin software or protocol, their authority to do so, and their resulting ability to implement their solution, is in question. This means that anyone with a suggested resolution to a crisis may merely propose a solution, but it may take too long to achieve buy-in from other members of the Bitcoin community to successfully implement the solution in an emergency situation. We see this type of argument commonly made in debates over the limits of the executive power of the President of the United States, who may need to act quickly in a crisis without waiting for specific authority from Congress.[155]

The inability to obtain buy-in to a change in the Bitcoin protocol or software may also be a problem in non-crisis situations, when the core developers feel that a certain change to the Bitcoin protocol or software is in society's best interest (e.g., if they decided that the cap on the number of total bitcoins needed to be changed). Because changes to the Bitcoin software are ultimately made through the adoption of the new software by users, some users could hold out, preventing needed changes. This may be a real problem with Bitcoin particularly, as many of its users believe strongly in the decentralization premise, and may be unwilling to agree to fundamental changes to Bitcoin—even if such changes would be beneficial to society. (Interestingly, during the publication cycle of this Article, this situation began to play out in real time through the block size debate described *supra* in Section III.A.3, which has manifested in a split in the core

154. *See infra* notes 161–64 and accompanying text.

155. *See generally* ERIC POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC (2011) (arguing a strong presidency is necessary in the modern world as the executive is often called upon to act quickly in a world of far more complexity than that of the Framers); Saikrishna Bangalore Prakash, *The Imbecilic Executive*, 99 VA. L. REV. 1361 (2013) (arguing that despite arguments to the contrary, the Constitution limits the President's ability to act unilaterally even in times of emergency).

developers on the trajectory of Bitcoin.[156] The situation remains unresolved as of this writing.)

Decentralization also threatens Bitcoin's continued operation because it means that no one has the authority to speak as "the voice" of Bitcoin.[157] In a decentralized organization, with no rights or rules, there is no way to determine what is in the "best interests" of Bitcoin. Although certain people have assumed the role of "the voice" of Bitcoin already, they have not done so with authority to represent the interests of all owners of bitcoins. For instance, both the core developers of the Bitcoin software and representatives of an organization called "The Bitcoin Foundation"[158] have met with many government regulators to explain and advocate for certain treatments of Bitcoin,[159] but none of these people have any official authority to represent Bitcoin or its community. Yet, these people have in many ways stepped up to become the "voice" of Bitcoin because regulators have sought to be educated about it, and had to talk to *somebody.*[160] Bitcoin's decentralized structure means that there cannot be an official voice of the organization, which is highly problematic in a world that needs to understand Bitcoin in order to evaluate its risks and benefits.

Decentralization also means that the people who comprise the Bitcoin community are always in flux. Nodes may freely enter and exit the Bitcoin peer-to-peer system, meaning that the composition of

---

156. *See supra* notes 137–39 and accompanying text.

157. *See About Bitcoin.org: Who Owns Bitcoin.org?*, *supra* note 23 ("[N]obody can speak with authority in the name of Bitcoin.").

158. The Bitcoin Foundation was created in July 2012 to advocate for the success of Bitcoin. *See Transparency*, BITCOIN FOUND., https://bitcoinfoundation.org/transparency/ (last visited Nov. 15, 2015). Since then, there has been much debate in the Bitcoin community over the role of the Bitcoin Foundation, and in the fall of 2014, the Foundation limited its mission to supporting the development of the Bitcoin core software. *See Everybody Pivots*, BITCOIN FOUND. (Nov. 19, 2014), https://bitcoinfoundation.org/bitcoin/everybody-pivots/ (describing the evolving goals of the Bitcoin Foundation, from "public policy, education and outreach, [and] core development" originally, to its current "focus on funding the ongoing core development" of Bitcoin).

159. *See* Brian Fung, *Inside the Bitcoin Advocates' Closed-Door Meeting with Federal Regulators*, WASH. POST (Aug. 27, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/27/inside-the-bitcoin-advocates-closed-door-meeting-with-federal-regulators/ (reporting on the meeting between members of the Bitcoin Foundation and representatives from the U.S. Justice Department, Federal Bureau of Investigation, Department of Homeland Security, Internal Revenue Service, Secret Service and the Financial Crimes and Enforcement Division (FinCEN) of the Treasury Department); Simonite, *supra* note 37.

160. *See Everybody Pivots*, *supra* note 158 ("In the beginning, the foundation did it all—public policy, education and outreach, core development—*primarily because there was no one else to do it*." (emphasis added)).

the group is difficult to pin down. This makes it even more difficult to determine who has authority to speak on behalf of Bitcoin, to determine what is best for Bitcoin and its users, or to make and implement decisions in the case of a crisis.

Operational crises are not merely far-fetched, "what-if" scenarios. Bitcoin has already experienced several software malfunctions that could have caused its collapse if not remedied by a coordinated effort of Bitcoin software developers and miners. For example, as discussed earlier, the March 2013 "hard fork" resulted in two separate forms of the blockchain being created by computers within the Bitcoin network, when the system's entire value is premised on the existence of a single, authoritative blockchain.[161] The developers realized that the fork had been caused by computers within the network using different versions of the Bitcoin protocol.[162] Bitcoin's much-vaunted "decentralization" was revealed to be incomplete, as the core developers were able to contact and persuade enough Bitcoin mining pools to take action to ensure that one ledger (as recommended by the core developers) survived and the second ledger did not.[163] This revealed that certain people within the Bitcoin community have power to make certain decisions that affect the operations of Bitcoin as a currency. Yet the parties who made these decisions were not selected through any official process (such as voting), and were in no way accountable for the outcomes of their actions. While a potential crisis was averted in the instance of the March 2013 hard fork, this does not guarantee that a decentralized structure will enable successful crisis management in the future.[164]

So, Bitcoin currently operates in a rather contradictory way—it is decentralized in some ways but not in others. The parties who act as the central authority within Bitcoin acknowledge their power in cer-

---

161. *See 11/12 March 2013 Chain Fork Information*, *supra* note 135.

162. VELDE, *supra* note 136, at 3.

163. *See* Gavin Andresen, *March 2013 Chain Fork Post-Mortem*, GITHUB: BITCOIN IMPROVEMENT PROPOSALS (Mar. 20, 2013), https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki (stating that "[miners] Marek Palatinus and Michael Marsee quickly downgraded their nodes to restore a pre-0.8 chain as canonical, despite the fact that this caused them to sacrifice significant amounts of money and they were the ones running the bug-free version"); *see also* GERVAIS ET AL., *supra* note 36, at 57 (describing the resolution of the blockchain fork and stating that the manner of resolution was "at odds with Bitcoin's claim that it's a decentralized system and that the majority of the computing power regulates its decisions").

164. Resolving the March 2013 fork required groups that held a significant percentage of the computing power used to mine Bitcoins to agree to support a particular version of the blockchain. *See* Andresen, *supra* note 163. This meant they had to act altruistically rather than in their own best interest and "sacrifice significant amounts of money." *Id.* Such altruistic acts cannot be presumed in the future.

tain situations, but not in others; because there is no "official" power structure, it is not possible to hold those in power accountable for their actions. This ambiguous status is troubling in many ways.

Why This Is a Problem for Bitcoin as Financial Market Infrastructure

Bitcoin's decentralized structure is particularly problematic given the potential of the Bitcoin blockchain to serve as financial market infrastructure. A decentralized structure creates the risks that *no one* will even attempt to ensure that Bitcoin works; that even if someone does step up to help, he or she has no official authority or ability to implement suggested fixes; that the crisis management process may be slowed because of the lack of authority or responsibility; and that it will be difficult to tell who should be involved in the process because the Bitcoin community is so fluid.

With existing centralized financial market infrastructure, it is at least clear who has the responsibility to manage and repair it, and it is possible to impose risk management obligations on *someone*. Indeed, global financial regulators set standards for financial market infrastructure that are targeted at the defined entities who own and operate them. As made painfully clear with the Heartbleed bug and as commentators have noted in other contexts, when no one has direct responsibility to perform a task, it may very well go unperformed, as people tend to assume that someone else will handle it.[165] Maintaining the functionality of financial market infrastructure is hugely important, and having no one specifically tasked with the responsibility for achieving this for Bitcoin is a significant risk.

C. Bitcoin as Open-Source Software

Bitcoin's status as open-source software also creates systemic operational risks that generate instability. I will first provide a brief explanation of what open-source software is, then move to explain the risks this structure raises for Bitcoin. This discussion is not intended to resolve the ongoing and impassioned debate on the merits of open-

165. *See* Perlroth, *supra* note 97 (quoting Columbia University computer science professor Steven. M. Bellovin as saying of the Heartbleed bug: "This bug was introduced two years ago, and yet nobody took the time to notice it. . . . Everybody's job is not anybody's job."); *see also* Andrew Meneely et al., *An Empirical Investigation of Socio-Technical Code Review Metrics and Security Vulnerabilities*, 2014 PROC. SIXTH INT'L WORKSHOP ON SOC. SOFTWARE ENGINEERING 37, http://dl.acm.org/citation.cfm?doid=2661685.2661687 (evaluating "Linus' Law" empirically and noting the negative impact of the "Bystander Effect" in the discovery of security vulnerabilities in open-source software).

source software generally,[166] but merely to acknowledge that its use does create operational risks for Bitcoin, particularly in the context of the Bitcoin blockchain's role as potential financial market infrastructure.

Open-source software is software that makes its "source code" (i.e., its human language instruction manual) freely available to the world.[167] Software that is open-source is made available to users through a license agreement that gives the user permission to alter the source code.[168] Open-source software is contrasted against "proprietary software," which is issued under a license agreement that forbids the licensee from making any changes to the software.[169] Software that is purchased from companies like Microsoft or Adobe is generally proprietary software.

The method of developing and maintaining open-source software is one of its defining attributes, and distinguishes it most sharply from proprietary software. Open-source software is developed in a collaborative, open way.[170] When the full source code is posted publicly for all to see, software developers take the initiative to craft improvements to the software, such as new features or fixes to problems.[171] They propose their changes publicly, and the code evolves over time.[172] Crucially, open-source software developers are usually not paid for their work; rather, it is generally done in developers' spare time and is viewed as an altruistic or reputation-enhancing activity.[173]

Open-source software is viewed by some as having many benefits over proprietary software. The collaborative ethos of the software creation process in open-source software is celebrated. Many state that open-source software is less vulnerable and more resilient than proprietary software, because the development of the software is transparent, and since more eyes are looking for bugs, more bugs will be noticed and fixed.[174] However, even open-source software is widely acknowl-

166. For an overview of the debate, see generally FADI P. DEEK & JAMES A. MCHUGH, OPEN SOURCE: TECHNOLOGY & POLICY (2008).
167. *See id.* at 1.
168. *See id.*
169. *Id.*
170. *See id.* at 162.
171. *See id.* at 5.
172. *See id.* at 163.
173. *See id.* at 162–63.
174. *See id.* at 5, 59–60. As famously stated by Eric Raymond in the seminal *The Cathedral and the Bazaar*, Linus's law is that "given enough eyeballs, all bugs are shallow" or "[g]iven a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix obvious to someone." Eric Steven Raymond, *Release Early, Release Often*, CATHEDRAL & BAZAAR (2000), http://

edged to be plagued with bugs, as a developer for Mozilla (a prominent open-source software that runs the web browser Firefox) stated in 2005 that "everyday, almost 300 bugs appear . . . far too much for only the Mozilla programmers to handle."[175] Indeed, as discussed in Section IV.A.1 of this Article, it is widely understood within the Bitcoin developer community (though not discussed much in the mainstream press) that there are ongoing problems with the Bitcoin code that require fixes.[176]

Leaving aside any debate over whether Bitcoin's open-source nature makes it less buggy or whether open-source is better than proprietary software generally, the open-source character of the development of Bitcoin's software and protocol creates important systemic operational risks for the Bitcoin blockchain. These include (1) the risk that no one will properly maintain the code because no one has the actual *responsibility* to do so; (2) the risk that conflicts of interest may shape the management of the Bitcoin code (and therefore financial market infrastructure itself); and (3) the risk that consensus on changes may be unachievable, leading to splits (or "forks") in the network. I will discuss each of these risks in turn.

Bitcoin's status as open-source software means that everyone interested *may* participate in the continued development and maintenance of the software, but, crucially, that no one *must* do so. This echoes some of the risks raised by Bitcoin's decentralized structure. As stated in Section III.B above, if no one *must* do it, there is no guarantee that it will be done, or that it will be done well. We see some of the tensions created by Bitcoin's open-source nature beginning to play out already, as the volunteer nature of the code maintenance and development is buckling under the weight of managing an ever more important project (its importance increasing with its more

---

www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ar01s04.html. *But see* GLASS, supra note 91 (arguing that there is no evidence that, once past a threshold small number of developers, more developers will either identify or resolve more software bugs). The recent Heartbleed and Shellshock bugs also tend to undermine Raymond's claim that all bugs will be found quickly in open-source software. *See supra* notes 92–98 and accompanying text.

175. Claire Le Goues et al., *The Case for Software Evolution*, 18 PROC. FSE/SDP WORKSHOP 205, 205 (2010), http://www.cs.cmu.edu/~clegoues/docs/legoues-foser10.pdf (internal quotation marks omitted) (quoting John Anvik et al., *Who Should Fix This Bug?*, 28 INT'L CONF. ON SOFTWARE ENGINEERING 361, 363 (2006)).

176. *See supra* notes 99–103 and accompanying text. Additionally, the Bitcoin Foundation has assessed the likelihood of certain threats to its software. On a scale of 1 to 7, the Foundation assesses the likelihood that "significant" bugs lurk in the Bitcoin protocol at around 4 and the likelihood that "significant" bugs lurk in the software code at more than 4.5. RISK MANAGEMENT STUDY, *supra* note 102, at 8.

widespread use, higher valuation, and the huge investments being made in the ecosystem surrounding it). For example, over the past year and during the publication cycle of this Article, the compensation of the team of core developers has shifted dramatically, accompanied by much debate.[177]

Moreover, the open-source nature of Bitcoin software development means that important repairs to the code are delayed because, until very recently, no one has had a full-time job—with full-time pay—to service the code.[178] Indeed, both the core developers and high-profile investors in companies providing Bitcoin-related products or services have raised alarms that the code development structure has delayed important necessary repairs to the Bitcoin code.[179] If core developers are not paid for their efforts on Bitcoin, they must have other sources of income. Thus, until recently, Bitcoin code maintenance and development have been only a hobby for these people to pursue in their spare time. Since they have had to fit code maintenance in before or after their real jobs, it is not surprising that crucial changes to the Bitcoin software have been slow.[180] Professional investors like the

177. *See Bitcoin Raises Its Profile but Investors Demand More*, IRISH TIMES (Aug. 4, 2014), http://www.irishtimes.com/business/bitcoin-raises-its-profile-but-investors-demand-more-1.1884918 (describing the debate within the Bitcoin community about how to fund the development of the core software); *Is Funding a Development Team Really That Difficult?*, BITCOIN F. (June 27, 2014, 2:13 PM), https://bitcointalk.org/index.php?topic=667926.0 (debating the need to provide additional funding for development of the Bitcoin software and the appropriate source of the funds); *see also* Nermin Hajdarbegovic, *Mike Hearn: Underfunding Is Leaving Bitcoin Development in Crisis*, COINDESK (June 25, 2014), http://www.coindesk.com/mike-hearn-underfunding-leaving-bitcoin-development-crisis/ (describing a leading Bitcoin software developer's concerns that "the core bitcoin system is radically underfunded and underdeveloped from where it needs to be").

178. *See Strengthening the Core*, BITCOIN FOUND. BLOG (Nov. 20, 2014), https://blog.bitcoinfoundation.org/strengthening-the-core/ (describing how the compensation of the core developers has evolved over time).

179. *See* Danny Bradbury, *Gavin Andresen to Bitcoin Companies: Support Open Source*, COINDESK (Feb. 21, 2014), http://www.coindesk.com/gavin-andresen-bitcoin-companies-support-open-source/ (reporting that Bitcoin core developer Gavin Andresen wrote to Bitcoin companies urging them to assist the core developers in developing, reviewing, and testing the code rather than treating the code like a purchased product); Hajdarbegovic, *supra* note 177 (reporting a software developer's concerns that "because developers are not incentivised [through pay] . . . they simply don't tend to tackle the big problems and little progress is being made"); Kadhim Shubber, *Jeremy Allaire: Bitcoin Developers Need to 'Step Up,'* COINDESK (July 2, 2014), http://www.coindesk.com/circle-ceo-jeremy-allaire-issues-challenge-bitcoins-core-developers/ (reporting that CEO of Bitcoin wallet company Circle calls for changes in the software development process to support the huge industry being built on top of the code).

180. As core developer Gavin Andresen wrote in a blog post on Bitcoin software development:

venture capitalists that have been piling in to Bitcoin over the last two years[181] are not used to having to wait for fixes to business problems—paying the party who can fix the problem to do it well and quickly is how professional business people operate. The maverick structure of Bitcoin software development has therefore been frustrating for the professional moneyed interests that have entered the Bitcoin ecosystem.[182]

These problems with adequate maintenance of the code due to its open-source status have spurred searches for fixes that, in turn, create other problems. Businesses and advocacy organizations within the Bitcoin ecosystem have recognized that the Bitcoin code needs more time and attention from the core developers, so they have started to pay the core developers for their work on Bitcoin. Over the course of Bitcoin's existence, the compensation of the core developers has evolved from no compensation, to compensation by private businesses within the Bitcoin ecosystem, to compensation by non-profit digital currency advocacy groups. As of this writing, several of Bitcoin's core developers are based in the Massachusetts Institute of Technology's Digital Currency Initiative, and are compensated by MIT.[183] It is unclear who is paying the remaining core developers (if anyone), but in the past, some of the core developers were paid by the nonprofit Bitcoin Foundation, while others were full-time employees of Bitcoin-focused businesses.[184] For instance, from May 2013 to December

---

> People are busy. They have lives, families, careers and hobbies outside of Bitcoin. It's unrealistic to put expectations of a full-time employee onto a volunteer. As more and more people come to rely on this protocol and businesses build products and services powered by Bitcoin, it becomes increasingly more important to have a dedicated team doing the painstaking work it requires.

Welcome Sergio Lerner!, BITCOIN FOUND. BLOG (Dec. 5, 2014), https://blog.bitcoinfoundation.org/welcome-sergio-lerner/.

181. *State of Bitcoin 2015: Ecosystem Grows Despite Price Decline*, COINDESK (Jan. 7, 2015), http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline/ (reporting that venture capital investment in Bitcoin-related companies totaled $433 million from 2012 to the end of 2014).

182. *See* Shubber, *supra* note 179.

183. *See* Brian Forde, *Welcome to the MIT Media Lab, Gavin, Wlad, and Cory*, MIT MEDIA LAB (Apr. 22, 2015), https://medium.com/mit-media-lab-digital-currency-initiative/welcome-to-the-mit-media-lab-gavin-wlad-and-cory-977ae418c084 (reporting that Gavin Andresen, Wladimir van der Laan, and Cory Fields, "three of the leading developers of the Bitcoin core project," had accepted positions at the Digital Currency Initiative).

184. *See Strengthening the Core*, *supra* note 178 (stating that three Bitcoin software developers are paid by the Bitcoin Foundation, one developer is paid by private company BitPay, and two developers are paid by private company Blockstream); *Welcome Sergio Lerner!*, *supra* note 180 (stating that the Bitcoin Foundation has hired Sergio Lerner as a new developer to focus on security testing of the Bitcoin code).

2014, core developer Jeff Garzik was a full-time employee of BitPay, a prominent business that facilitates businesses' acceptance of bitcoin payments.[185]

This compensation of the core developers may be necessary to adequately maintain the code, but it raises clear conflicts of interest. If a developer is paid by a particular business to do work on a communal, public project like Bitcoin, the developer has a strong incentive (i.e., a paycheck) to prioritize his employer's interests over the interests of the Bitcoin community as a whole. One could imagine a scenario in which a developer's employer had a different interest than other Bitcoin owners; the developer may choose to further his or her employer's interest over other Bitcoin owners, with no official accountability to anyone. This plays out not just through changes made to the Bitcoin software code but also in the ways that the core developers interact with regulators, businesses, and media, as the core developers have been sought out as the "voices" of Bitcoin.[186] The messages that the core developers convey to outside parties may benefit or harm some bitcoin owners more than others. A quick skim of the Bitcoin Internet forums reveals that bitcoin owners have different ideas about what is beneficial for the currency,[187] and the conflicts of interest carried by the core developers may certainly impact their behaviors and decisions regarding Bitcoin.

Finally, the mode of open-source software development means that consensus to proposed changes to the code may be difficult to achieve. As of this writing, this problem is playing out through a heated debate over the appropriate "block size."[188] A technical point (how much computer memory a "block" should consume) that has real implications on the costs and power dynamics of the network,[189] this

185. *See* Elizabeth Ploshay, *BitPay Hires Jeff Garzik*, BITCOIN MAG. (May 15, 2013), http://bitcoinmagazine.com/4515/bitpay-hires-jeff-garzik/. According to Mr. Garzik's LinkedIn page, he worked for Bitpay until December 2014. *See infra* note 194.

186. *See supra* notes 157–60 and accompanying text.

187. *See, e.g.*, *Topic: How Could Bitcoin Evolve?*, BITCOIN F. (Oct. 3, 2014, 6:52 PM), https://bitcointalk.org/index.php?topic=809588.0 (debating ending proof of work (Pow) as part of Bitcoin mining, among other matters); *Topic: The Problem of Centralized Develpoment ("Core Devs") in Bitcoin*, BITCOIN F. (Oct. 22, 2014, 5:42 PM), https://bitcointalk.org/index.php?topic=831540.0 (debating whether the Bitcoin core developers should simply implement the wishes of the Bitcoin community as expressed through votes or should also make policy decisions that they implement in the code).

188. *See supra* note 137–39 and accompanying text.

189. This debate has money and power implications, because the size of a block determines how much memory a computer has to devote to storing copies of the blockchain, or ledger. The system creates its "distributed trust" through multiple cop-

debate is emblematic of the important policy choices embedded in every change to the software—whether they seem purely technical or not. The core developers have split into different factions on this point, and the debate threatens to similarly split the network,[190] raising questions about the value of the "bitcoins" embedded in each surviving network and how financial market infrastructure or a business ecosystem balanced on top of a severed series of networks would operate. Even if the block size debate is resolved without a "fork," there are infinite other serious technical (and therefore policy) issues that could fracture the network, making this a significant operational risk.

Why This Is a Problem for Bitcoin as Financial Market Infrastructure

While problems like inadequate code maintenance, conflicts of interest among code developers, or failure to obtain consensus to software changes may not be of great significance in a typical open-source software project, such as one that creates a web browser (like Firefox) or a computer operating system (like Linux), they are of grave importance in software whose functioning undergirds financial market infrastructure. Financial market infrastructures such as money and payment systems act in many ways as public goods,[191] making the risk of failure due to an overlooked software glitch, conflicts of interest with a private employer, and a fractured network due to failed consensus on a software change highly problematic. The operation of financial market infrastructures is critical to financial stability, hence their strict regulation, which includes both governance and risk-management requirements.[192] Leaving fixes to financial market infrastructure to be remedied by a hobbyist who has no accountability (other than reputation) to do the repair correctly or in a timely manner, or who may be incentivized by a paycheck to act on behalf of his or her private employer rather in the interests of the public, is a high-risk way to operate these vital structures.

Both sides of the coin are problematic here: either Bitcoin adheres to traditional, open-source, decentralized practices of maintaining the software through purely volunteer contributions, resulting in

---

ies of the blockchain spread throughout the network. Computer memory costs money; money determines who is able to afford to participate in the network. The more money it costs to participate, the fewer "nodes" or "miners" there will be in the network (or the more concentrated mining pools become), meaning the network can become more and more centralized as it becomes cost-prohibitive to participate.

190. *See* Caffyn, *supra* note 137.

191. Ferrarini & Saguato, *supra* note 69, at 583 ("In particular, policy makers stressed the importance of public regulation in modeling prudential and corporate governance standards for FMIs, given the 'public' nature of their services.").

192. *See supra* Section II.B.

inadequate code maintenance and higher risk of software problems or it tries to do better software maintenance by having private parties compensate core developers for their work, introducing conflicts of interest into the mix. Either scenario is worrisome if the Bitcoin blockchain serves as financial market infrastructure. In spite of the "open" nature of open-source software, its development methods, coupled with the decentralized structure of Bitcoin, create significant operational risks.

D. Bitcoin's Expertise Problem

The final operational risk that I will discuss in this Article is what I term the "expertise problem." This is the risk that springs from people with predominantly technical (computer or software) expertise operating and controlling an item that has, in recent history at least, been maintained and controlled by parties who at least purport to have some education and expertise related to money or finance.[193]

Software coders, who make the decisions about what the Bitcoin software will look like and what functions the system will have, are not necessarily financial systems experts. The known backgrounds of the core team of developers are in computer science and software development, not in economics, finance, financial systems, or monetary policy.[194] Examples of decisions that have been made by the software

---

193. Eric Posner referred to this expertise problem in his piece for the *New Republic* in December 2013:

> In response to those who have argued that bitcoin is inherently deflationary because the supply does not grow as rapidly as the global economy—which encourages hoarding of money rather than its use for investment—one commentator pointed out that the "bitcoin community" can increase the supply of bitcoins through majority rule by jointly reprogramming the underlying software, which is publicly accessible. But if this is true, it means that bitcoin is controlled by a central bank after all, albeit one whose boardroom holds millions of people. The money supply is determined by votes cast by people who know nothing about monetary economics and little about the economic conditions that justify modification of it. So on what basis would they decide to increase the supply of the currency, and by how much?

Eric A. Posner, *Bitcoin's Bandwagon Has Never Been More Crowded*, NEW REPUBLIC (Dec. 3, 2013), http://www.newrepublic.com/article/115801/bernankes-bitcoin-comments-signal-growing-acceptance; *see also* Yermack, *supra* note 55, at 5 (noting that "macroeconomic policy decisions [about Bitcoin could end up] controlled by an online discussion forum or blog rather than by an expert agency such as the Federal Reserve").

194. For profiles on core developers, see Gavin Andresen, LINKEDIN, https://www.linkedin.com/in/gavin-andresen-6987971 (last visited Nov. 9, 2015); Jeff Garzik, LINKEDIN, https://www.linkedin.com/in/jeffgarzik (last visited Nov. 9, 2015); Pieter Wuille, LINKEDIN, https://www.linkedin.com/in/pieterwuille (last visited Nov. 9, 2015); *see also* Simonite, *supra* note 37 (describing Gavin Andresen's background

developers (including the original developer, Satoshi Nakamoto) include: having a cap on the number of Bitcoins that may ultimately be issued, having Bitcoins be divisible into a certain number of smaller chunks, reflecting all transactions on a common ledger that is distributed amongst Bitcoin nodes, the trajectory of Bitcoin, and how Bitcoin should interact with government regulators. There are no doubt countless others. All of these decisions impact the viability and success of the Bitcoin blockchain as financial market infrastructure, and all have been made by software developers rather than financial systems experts.

Why This Is a Problem for Bitcoin as Financial Market Infrastructure

If a crisis related to Bitcoin's operation or value should arise, there are no financial systems or payments experts who would *necessarily* be involved in reacting to the crisis. The computer experts would be the primary first responders, and would rely on their own backgrounds to determine the appropriate response. This is what happened with the March 2013 fork in the Bitcoin blockchain, when the core developers coordinated a response to resolve the matter.[195] This is not to say that experts in one field cannot succeed in another (indeed, I seek to point out some problems with Bitcoin itself from a non-expert's perspective) but that with something as important as financial market infrastructure, it seems to make sense to have people with an in-depth understanding of the world financial and monetary systems as a whole, involved in making decisions about how it operates. To pretend that with Bitcoin, *no one* makes these decisions—or that the computer coders who manage Bitcoin are not making policy choices with critical implications—is both false and dangerous.

The creation of financial systems infrastructure by non-experts, as is the case with Bitcoin and other virtual currencies, aligns with the trend of production by non-experts that is widely recognized and discussed in Internet and media circles.[196] Bitcoin represents an exten-

---

in computer science and software development). Neither Gregory Maxwell nor Wladimir J. van der Laan appear to have a LinkedIn profile or other publicly available profiles.

195. *See supra* notes 161–64 and accompanying text.

196. *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006) (discussing the social benefits of peer production versus centralized production); LESSIG, *supra* note 3 (discussing the cultural shift toward nonprofessionals contributing creatively to information development and the economic structure). This trend is best demonstrated by the widespread creation of media content by individuals as opposed to more centralized sources. Professor Lawrence Lessig has referred to this as a transition from a primarily "Read Only" world to one which is also "Read-Write," where the masses do not

sion of this trend of decentralized amateurs seizing control of the creation of a product from centralized sources deemed to have power and expertise.[197] While this movement of amateur creation has generated amazing creative content, and is laudable in many ways, there are certain products or things that pose risks that demand they be produced or managed by those with relevant expertise or authority. As even Lawrence Lessig, an avid supporter of open-source software and the peer production movement, has acknowledged, "There are places where authority is required: No one should want Congress's laws on a wiki. Or instructions for administering medication. Or the flight plan of a commercial airliner."[198]

Financial market infrastructure, with its important social functions, is one of these places. Just as certain areas like flight plans and medication dosages require *authority* to rely upon, given the dire consequences of errors in these matters, so too do these areas require *expertise*. Functioning financial market infrastructure benefits everyone who uses it, and users of a particular payment system or central clearinghouse are crippled if it stops working. A high level of expertise in money, finance, financial systems, and economics, rather than just the technical or mechanical processes that operate the infrastructure, is essential in those running the system, given the important policy choices that the Bitcoin developers are making through their code.

As Part III has demonstrated, the Bitcoin blockchain is subject to significant operational risks, primarily related to its technology and governance issues, which impact its reliability as financial market infrastructure.

IV.
Why Aren't We Talking More About Bitcoin's Operational Risks?

The operational risks of Bitcoin have not gone unnoticed, but they have received far less attention than the harms that might be caused by Bitcoin's use. Thus far, regulators have primarily focused their attentions on categorizing Bitcoin under existing laws, identifying and halting the harms that Bitcoin's use can facilitate (e.g., the

just consume (or "read") content, but actively create (or "write") it themselves. Lessig, *supra* note 3, at 84–85. Rather than content coming solely from record labels, movie studios, or mainstream newspapers, it comes from individually made recordings that people post on YouTube, websites, or blogs.

197. See Vigna & Casey, *supra* note 53, at 276–78 for a description of the trend toward amateur control of traditionally centralized product and service markets.

198. Lessig, *supra* note 3, at 84–85.

operation of illicit online marketplaces like Silk Road or money laundering), and regulating the businesses that operate the Bitcoin ecosystem, such as exchanges and wallet companies.[199] Only relatively recently have regulators and scholars begun to talk more about the operational risks of Bitcoin in their public writings. For example, within the last eighteen months, the European Central Bank and the European Banking Authority wrote about the technology and governance risks associated with virtual currencies.[200] Two recent computer science papers have also opened a more in-depth analysis of Bitcoin's operational risks.[201] In general, however, while there have been references and short discussions related to Bitcoin's operational risks in academic or U.S. regulatory writings, these are few compared to the extensive writings on Bitcoin's "use" risks.[202]

---

199. For a regularly updated compilation of regulatory actions on virtual currencies, see Davis Polk & Wardwell LLP, *Virtual Currency Regulation Resources*, BITCOIN-REG.COM, http://bitcoin-reg.com/ (last visited Oct. 23, 2015) (highlighting actions by the Internal Revenue Service, Commodity Futures and Trading Commission, Securities and Exchange Commission, FINCEN, and other money transmission and consumer protection regulators).

200. In February 2015, the European Central Bank noted that Bitcoin's open-source software development process means that "no single entity [is] responsible for preventing or resolving [major] incidents." 2015 ECB PAPER, *supra* note 38, at 20. It noted:

> Like any highly IT and network-dependent mechanism, [virtual currencies] are specifically subject to operational risks. These include a wide spectrum of risks, ranging from technical failures to hacking, without obligations to mitigate these risks as is the case for financial institutions and payment systems. Those failures or hacking attacks can occur at individual level (loss or theft of private cryptographic keys or user credentials) or on a wider scale (disruption to, or hacking of, the technical infrastructure of the key actors).

Id. at 22; *see also* EUROPEAN BANKING AUTH., EBA OPINION ON 'VIRTUAL CURRENCIES' 38 (2014), https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (identifying operational risks of virtual currencies, such as the fact that the software operating the currency can be changed, "accidently introduc[ing] errors" or being done without "good faith;" the fact that "the operator of a [centralized] virtual currency may lack adequate and secure IT infrastructure and governance arrangements . . . or [fail to] act with sufficient integrity;" and a "lack of corporate capacity and governance: lack of skills, expertise, systems, controls, organizational structure and governance exercised by market participants").

201. *See* KIRAN & STANNETT, *supra* note 86; PETERS ET AL., *supra* note 86.

202. *See, e.g.*, VELDE, *supra* note 136, at 3 (hinting at operational risks of Bitcoin in its discussion of blockchain forks, continued maintenance of the code by "a small set of programmers," and "incentives to hijack" Bitcoin); Grinberg, *supra* note 39, at 175–76, 179–81 (providing a brief discussion of "potential technology failures" of Bitcoin, including failure of anonymity associated with the currency, theft of bitcoins from users, and DDOS attacks on the Bitcoin system and noting that the developers of the Bitcoin software may make changes to it that could undermine confidence in the currency); Reber & Feurstein, *supra* note 59, at 91–92 (noting in passing that Bitcoin is subject to "operational risk, the risk that arises through the reliance on the function-

In general, regulators' consideration of Bitcoin has focused on questions like, "What bad things does Bitcoin allow people to do?" and "How does Bitcoin fit under existing law?" without fully resolving questions like, "What is it?" and "How is it made to work reliably?" In this Article, I seek to take a step back to ensure that we are fully cognizant of, and comfortable with, our management of the more fundamental operational risks of Bitcoin in considering its blockchain as potential financial market infrastructure.[203]

There are a number of possible reasons why the operational risks of Bitcoin have received less attention from regulators or commentators. These reasons may include:

(1) Bitcoin and other virtual currencies have been viewed as too insignificant or outside the mainstream to warrant concern with the robustness of their ongoing operation;

(2) Bitcoin's operational risks are viewed as too obvious, minor, or boring to merit extended discussion;

(3) Bitcoin is seen, or at least described, by many of its proponents as a perfect, organic product, rather than a product created and managed by humans;

(4) regulators and society in general have grown comfortable with computer software playing an integral role in our lives, and even with the sharing or open-source models of creating and maintaining the software;

(5) "techno-fundamentalism"; and

(6) a belief that innovation is inherently positive and we must give innovation the chance to demonstrate its full benefits before condemning or shutting down innovative practices.

I will take each of these possible reasons in turn and discuss why they are insufficient reasons to gloss over Bitcoin's operational risks.

---

ing of the Bitcoin network"). Interestingly, the Bitcoin Foundation, a Bitcoin advocacy organization, published a lengthy list of threats to Bitcoin's success, including operational risks. *See* RISK MANAGEMENT STUDY, *supra* note 102, at 1, 2, 6–19.

203. Sarah Jane Hughes and Stephen T. Middlebrook hint at these issues:

> Proponents can't easily explain what a cryptocurrency is. If you can't explain what you are and how you fit into the current legal and regulatory scheme, you are at the mercy of the ignorant. The "what this is" answer needs to address not just things like "is it money transmission?" but more mundane yet important questions like "where is a bitcoin located?" and "where and when does a transaction take place?"

Sarah Jane Hughes & Stephen T. Middlebrook, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813, 839 (2014).

A. Bitcoin Is Too Small to Matter

Bitcoin has been dismissed by many as irrelevant, with its circle of use limited to a relatively small group of people. Writings by regulators have also perceived its narrow use, noting how the number of daily Bitcoin transactions pales in comparison with the number of daily non-cash transactions.[204]

Based largely on this limited use, certain regulators concluded that Bitcoin did not pose a risk of harm to the larger economy. If Bitcoin is used by only a few people, the argument goes, then only those few will be hurt if it fails, so why worry about whether Bitcoin works properly or not?[205]

For a while, this was a reasonable position to take, but I argue that the moment for dismissing Bitcoin as a fad has passed. Too many well-known, credible people are singing its praises and investing huge sums of money to build the Bitcoin and other virtual currency ecosystems.[206] Moreover, in the fall of 2012, when the European Central Bank (ECB) provided the initial global regulatory guidance on Bitcoin, there were only around 10,000 users of Bitcoin.[207] By contrast, in early November 2015, the *Financial Times* reported that more than 120,000 transactions are added to the Bitcoin blockchain every day."[208] Bitcoin therefore represents a much greater threat than it did previously, and for this reason regulators need to more explicitly factor Bitcoin's operational risks into their evaluation of Bitcoin.[209]

---

204. *See* 2015 ECB PAPER, *supra* note 38, at 16–17.

205. *See, e.g.*, 2012 ECB PAPER, *supra* note 38, at 6, 7 (noting that virtual currencies "cannot jeopardise financial stability, owing to their limited connection with the real economy, their low volume traded and a lack of wide user acceptance" and that "[o]wing to the small size of virtual currency schemes, these risks do not affect anyone other than users of the schemes").

206. *See supra* notes 6–13 and accompanying text.

207. *See* 2012 ECB PAPER, *supra* note 38, at 25.

208. Wild et al., *supra* note 61. Of course, as the ECB has noted, this number is still miniscule compared to the "274 million non-cash retail payment transactions per day for the EU only." 2015 ECB PAPER, *supra* note 38, at 17.

209. In 2012, the ECB noted that it would have to continue to reevaluate the risk posed by virtual currencies. 2012 ECB PAPER, *supra* note 38, at 7 ("[The risk] assessment could change if usage increases significantly, for example if it were boosted by innovations which are currently being developed or offered. As a consequence, it is recommended that developments are regularly examined in order to reassess the risks."). In its 2015 report, the ECB noted that "[a]s in 2012, again because of their small size, [virtual currencies] do not pose a threat to payment system stability." 2015 ECB PAPER, *supra* note 38, at 27. However, it noted that this could change depending on how integrated mainstream financial players become with virtual currencies and whether there is "a significant increase in users and the volume of transactions" in virtual currencies. *Id.* Further, the ECB acknowledged that virtual currencies "do have

B. Bitcoin's Operational Risks Are Obvious, Minor, or Boring

It is obvious that Bitcoin is decentralized, open-source software. It is also obvious that it is operated by people other than celebrated financial systems experts. These facts about Bitcoin are prominently displayed in virtually all descriptions of it, from the website www.bitcoin.org that seeks to educate the public on Bitcoin[210] to the white paper written by Satoshi Nakamoto[211] to the Bitcoin Foundation's website and materials.[212] These attributes of Bitcoin are not secrets, so perhaps everyone discussing Bitcoin's risks is already factoring them into their own risk analysis without the need to belabor them.

But, sometimes it is worth stepping back and more deeply considering the fundamental attributes of something when assessing its risks. When the securitization of subprime mortgages was in full swing during the mid-2000s, it would have been helpful if more people creating and purchasing mortgage-backed securities had considered that a basic attribute of a subprime mortgage was that it was issued at a subprime interest rate *because the borrower was a significant credit risk*—and that that inherent risk needed to be factored into both the rating and pricing of the aggregated mortgage-backed security. Just because the risk that many mortgages would be defaulted on simultaneously seemed low, the high consequences of it were discounted. It is just these types of risks—low likelihood, high consequence ones—that Nassim Nicholas Taleb argued that we tend to inappropriately discount in the seminal *Black Swan*,[213] and that I seek to ensure we are not doing now with our evaluation of Bitcoin and other virtual currencies.

C. Bitcoin Is Organic and Untainted by Human Hands

> *We have elected to put our money and faith in a mathematical framework that is free of politics and human error . . . .*
>
> —Tyler Winkelvoss, as reported in the *New York Times*[214]

---

the potential to have an impact on monetary policy and price stability, financial stability and the smooth operation of payment systems." *Id.* at 29.

210. Bitcoin Project, http://www.bitcoin.org (last visited Oct. 25, 2015).

211. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008) (unpublished white paper).

212. Bitcoin Found., https://bitcoinfoundation.org/ (last visited Mar. 12, 2015).

213. *See generally* Nassim N. Taleb, The Black Swan: The Impact of the Highly Improbable (2d ed. 2010).

214. Popper & Lattman, *supra* note 1, at A3. The quoted statement was made by Tyler Winklevoss.

If no-one owns it, how can I trust it?

. . .

In short, if you trust mathematics, you can trust Bitcoin.

—Multibit.org[215]

These statements have been put out into the world by proponents of Bitcoin, and they suggest to those who receive them that Bitcoin is somehow flawless and perfect—more of an elegant math theorem that follows the laws of science or nature rather than an invention of man. According to Tyler Winklevoss, a prominent Bitcoin supporter, Bitcoin is "a mathematical framework that is free of politics and human error."[216]

This type of messaging suggests that no person is responsible for Bitcoin itself—for the software's fundamental attributes (e.g., its limit on the total number of bitcoins that may be generated, how bitcoins are produced, making the software open-source and peer-to-peer, etc.) or for its continued operation or maintenance. It gives the impression that Bitcoin, like a math equation or a naturally occurring phenomenon like a flower, just *is*. Humans, with all of their foibles and flaws, did not make and do not make decisions about Bitcoin's fundamentals—Bitcoin operates because it is just math.

Perhaps these types of statements are meant to be taken with a grain of salt, or perhaps they stem from enthusiasm about Bitcoin by its proponents, but they are fundamentally inaccurate and potentially dangerous messages. Ordinary people created and maintain Bitcoin, and those facts make Bitcoin subject to human error—witness the long list of bugs that the Bitcoin developers themselves post publicly.[217] Bitcoin is subject to politics as much as any other human endeavor—witness the debates over its future in the Bitcoin message boards,[218] the important role the core developers play in determining its future,[219] and the potential conflicts of interests raised by the core developers' sources of income.[220] Witness the power struggle ongoing between the grownup, moneyed interests coming into the Bitcoin ecosystem through venture capital investments, and the early adopters who were or are interested in Bitcoin as a cool computer project or a

215. *See Frequently Asked Questions*, *supra* note 2.
216. Popper & Lattman, *supra* note 1, at A3.
217. *See generally Issues List*, *supra* note 99.
218. *See generally* BITCOIN F., https://bitcointalk.org (last visited Oct. 25, 2015).
219. *See supra* notes 32–37, 161–64, 178–90 and accompanying text.
220. *See supra* notes 183–87 and accompanying text.

realization of the dreams of Austrian economics.[221] Bitcoin is inescapably a *people* project, and, like all such projects, is flawed in certain ways.

D. We Are Comfortable with Software and Technology

Another reason why these operational risks may be discounted is that we as a society have become comfortable with the large role that software or other digital products play in our lives, and we have even become comfortable with open collaboration or open-source software models. If we are comfortable with software running our phones, photos, security systems, cars, and so many other fundamental pieces of our lives, why should we care if a new type of software is used to run our financial market infrastructures? Aren't all of them electronic already?

This may be a natural response in today's hyper-digital world, but we must remember that Bitcoin is not just any old software, and financial market infrastructure is systemically important in a special way. As discussed in Part III, Bitcoin's governance risks only exacerbate its technology risks, meaning that we must be extremely careful of the weight we expect the Bitcoin blockchain to bear. Systemically important financial market infrastructures may well be too heavy to run on top of the Bitcoin network.

E. "Techno-Fundamentalism"

"Techno-fundamentalism," a term coined by cultural historian Siva Vaidhanathan,[222] may also explain why Bitcoin's operational risks have received less attention from regulators and academics. "Techno-fundamentalism" refers to a "blind faith in technology," which Vaidhanathan used to describe the ethos of Google.[223] He notes that:

> The particular kind of hubris that energizes Google is the notion that you can always invent something to solve the problem that the last invention created. That's techno-fundamentalism. . . . Techno-fundamentalism assumes not only the means and will to triumph over adversity through gadgets and schemes but also the sense that

---

221. *See* VELDE, *supra* note 136, at 3–4 (noting that "much of the interest in Bitcoin" is inspired by the ideas of Friedrich Hayek of the Austrian School of Economics).
222. *See* VAIDHYANATHAN, *supra* note 4, at 75–76.
223. *Id.* at 75.

> invention is the best of all possible methods of confronting problems.[224]

In describing Google, Vaidhanathan wrote:

> Google works so well, so simply, and so fast that it inspires trust and faith in its users. As the science fiction writer Arthur C. Clarke famously wrote, "Any sufficiently advanced technology is indistinguishable from magic." And of course trust in magic, or suspension of disbelief, is a central part of the process of embracing the deific. That's why so much of what we say and write about the experience of Google sounds vaguely religious.[225]

Techno-fundamentalism also seems to be related to overlooking the human element in technology:

> [A]t its root is the black box of technological design. Although consumers and citizens are invited to be dazzled by the interface, the results, and the convenience of a technology, they are rarely invited in to see how it works. Because we cannot see inside the box, it's difficult to appreciate the craft, skills, risk, and brilliance of devices as common as an iPod or a continuously variable transmission in an automobile.[226]

Vaidhanathan's concept of techno-fundamentalism seems an apt description of much of the exuberance and passion we have seen Bitcoin proponents use to describe it, as well as the tendency to ignore the very human problems involved in governing the software code. The message that a techno-fundamentalist might have about financial market infrastructure is that all of its problems can finally be solved through the use of technology and math—virtual currencies such as Bitcoin represent that solution. From the Winklevoss twins, to venture capitalists, to the Bitcoin entrepreneurs who crowd the Bitcoin conferences and meetups now held around the globe, Bitcoin proponents are confident that Bitcoin represents a transformative and positive step forward in the evolution of financial systems.[227] It is the plodding

224. *Id.* at 76.

225. *Id.* at 53 (quoting ARTHUR C. CLARKE, 3001: THE FINAL ODYSSEY 36 (1997)).

226. *Id.* at 52.

227. *See, e.g.*, *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currency: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 113th Cong. 5 (2013) (statement of Patrick Murck, General Counsel, Bitcoin Foundation), http://www.hsgac.senate.gov/download/?id=4cd1ff12-312d-429f-aa41-1d77034ec5a8 ("[W]e believe Bitcoin holds out a number of powerfully beneficial social and economic outcomes, including global financial inclusion, enhanced personal liberty and dignity, improved financial privacy, and a stable money supply for people in countries where monetary instability may threaten prosperity and even peace."); JERRY BRITO & ANDREA CASTILLO, MERCATUS CTR., BITCOIN: A PRIMER FOR POLICY-MAKERS (2d ed. 2013), https://coincenter.org/wp-content/uploads/2013/08/Brito_BitcoinPrimer_v1.3.pdf (identifying Bitcoin's benefits as including "lower

Luddites (and the killjoy academics) like myself who are left to sound the notes of caution as the technology moves forward.

F. Let a Thousand Virtual Currencies Bloom

The final reason I'll discuss for why we might not be addressing the operational risks of Bitcoin is a belief that innovations need to be encouraged and allowed to flourish rather than being shut down. This is different than the worship of technology that defines "techno-fundamentalism" and seems to be afoot with regulators' treatment of Bitcoin. Indeed, Janet Yellen, Chair of the Board of Governors of the Federal Reserve System, recently noted:

> The costs and benefits of developing new statutes or regulations related to digital currencies should be weighed carefully. New regulation, such as the creation of special licenses for digital currency providers, may work to strengthen the soundness of virtual currency schemes and increase public trust in the products, as some may refrain from investing in or using digital currencies due to a perceived legal uncertainty and/or lack of consumer protection. On the other hand, new regulation would need to be flexible enough to address effectively the evolving nature of digital currency systems and technology *while not stifling innovation*.[228]

A separate presentation on virtual currencies given by an economist of the Boston Federal Reserve stated, "Longstanding Federal Reserve position on virtual currency [was that] regulators should be careful not to inhibit experimentation and growth of innovative payment technologies. . . ."[229]

U.S. regulators have been wary of reflexively outlawing Bitcoin and other virtual currencies.[230] There have been numerous warnings given by Bitcoin proponents that Bitcoin has created and will create many, many jobs, and that the United States stands to drive these jobs

---

transaction costs," "potential to combat poverty and oppression," and "stimulus for financial innovation"); Andreessen, *supra* note 65; Popper & Lattman, *supra* note 1.

228. Letter from Janet Yellen, Chair, Fed. Reserve Sys., to Congressman Mick Mulvany 8 (Sept, 4, 2015) (emphasis added), http://bitcoin-reg.com/sites/default/files/283714666-janet-yellen-response-to-us-representative-mick-mulvaney-on-bitcoin_0.pdf (responding to a question regarding whether she thinks new regulations are needed for Bitcoin and other virtual currencies).

229. OZ SHY ET AL., FED. RES. BANK BOS., CAN ECASH & VIRTUAL CURRENCY COMPETE WITH OTHER ELECTRONIC PAYMENTS? 12 (2014).

230. *See* CONFERENCE OF STATE BANK SUPERVISORS, CSBS POLICY ON STATE VIRTUAL CURRENCY REGULATION 1 (2014) ("State regulators recognize the public interest in allowing [virtual currency] technologies to develop in a purposeful manner, providing clarity and certainty for implementation, and ensuring the stability of the larger financial marketplace.").

abroad if it over-regulates virtual currency.[231] Regulators appear to be heeding these warnings and to be working to understand virtual currencies before they regulate.[232] Indeed, a bill was filed in Congress in December 2014 that would ban U.S. states and municipalities from regulating cryptocurrencies for a period of time to allow them to develop.[233]

This is generally a laudable position to take, as regulators certainly do not want to be accused of constricting innovation and job growth. However, this guiding principle should not blind them to important structural risks embedded in new technologies, particularly when these new technologies are attracting significant investment and attention from prominent business and policy leaders.

Conclusion

New technologies like Bitcoin always challenge our existing ways of thinking. What do we do with innovations that fundamentally alter key aspects of the way we live? Do we let them grow and see what benefits come of them, or do we try to anticipate their strengths and weaknesses and steer development to protect ourselves?

Financial market infrastructures form the circulatory system of our modern economies, and their failures can threaten financial stability. We should therefore scrutinize innovations that radically reshape these structures to make sure we are comfortable that they are robust enough to last. It is true, of course, that our current financial market infrastructures are fragile or flawed in their own ways. But, we should not overlook important operational risks as we glimpse opportunities to improve upon existing structures.

In this Article, I have sought to illuminate important technology and governance risks that could impact Bitcoin's ongoing operation and therefore the operation of any financial market infrastructure that

---

231. *See* Brito & Castillo, *supra* note 227; Andreessen, *supra* note 65; Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, The Private Digital Currency, and the Case Against its Regulation*, 25 Loy. Consumer L. Rev. 111, 171 (2012) ("Allowing bitcoin to operate unfettered by substantial regulation allows it to contribute towards job creation, economic growth, and opportunity.").

232. *See, e.g.*, *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currency: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 113th Cong. 1 (2013) (Senate hearing on virtual currencies); Fung, *supra* note 159 (reporting on a meeting with Bitcoin representatives and officials from multiple federal agencies); Joseph Young, *Financial Action Task Force Issues Bitcoin Guidelines, Warns about Money Laundering*, Bitcoin Mag. (July 1, 2015) (reporting on the work of an intergovernmental task force on digital currencies).

233. Cryptocurrency Protocol Protection and Moratorium Act, H.R. 5777, 113th Cong. (2014).

uses its blockchain. The amalgamation of Bitcoin's vulnerability to bugs, attacks, and uneven adoption of new releases, coupled with the governance problems that stem from its decentralized, open-source nature, must factor into the analysis of whether the Bitcoin blockchain is reliable. From my perspective, this package of risks, taken as a whole, makes Bitcoin too unreliable to support financial market infrastructure.

Given that significant resources are being devoted to Bitcoin and its surrounding ecosystem, as well as financial market infrastructures that will rely on it, it is vital to evaluate these risks now, to avoid building important structures on shaky foundations. While the harms that a Bitcoin blockchain failure would cause right now are relatively limited (particularly in comparison to what a collapse of an existing major payment system or clearing house would cause), the more structures that come to rely on the Bitcoin blockchain, the greater the global harms (and the waste of resources) will be.

Further, the analysis in this Article is relevant to the existing debate on whether open-source software, with its historically uncompensated and unaccountable software development process, is suitable for other types of critical public-focused infrastructures or practices, such as electronic voting, emergency management, national security, air traffic control, or weapons systems. If the open-source development process is problematic for Bitcoin in its role as financial market infrastructure because of the lack of accountability and conflicts of interest that can arise with the compensation of coders, then it may be similarly problematic for other critical public infrastructures. This is an area for further research.

We have watched before as massive structures in the financial industry were built on faulty foundations, and have all paid the price when those structures inevitably collapsed.[234] Let us hope that we have learned the lesson to attend to embedded risks as we are shaping new structures now.

234. *See* PATTERSON, *supra* note 146.

SECURITIES, INTERMEDIATION AND THE BLOCKCHAIN – AN INEVITABLE CHOICE BETWEEN LIQUIDITY AND LEGAL CERTAINTY?

Philipp Paech*

Abstract: *The practice of securities holding, transfer and collateral has significantly changed over the past 200 years –moving from paper certificates and issuer registers to an intermediated environment, and from there to computerisation and globalisation. These changes made transacting more efficient and thus rendered markets more liquid. However, the law has lagged behind and is now itself an obstacle to efficiency because international securities transactions are subject to considerable legal uncertainty. The latest global market development, a cryptographic transfer process commonly called 'the blockchain', is the most recent efficiency-enhancing change. It offers a unique possibility to create a consistent legal framework for securities from scratch, on the basis of a legal concept that to some extent resembles bearer securities. This paper shows what the new international legal framework could look like, in the light of experience gained from earlier developments.*

* Assistant Professor, Law Department, The London School of Economics and Political Science. I am grateful to Dan Awrey, Roy Goode, Hans Kuhn and Andrew Murray for their most helpful comments on an earlier draft of this article. All remaining errors are my own. The earlier version of this working paper was entitled 'Capital Markets Union, Investment Securities and the Tradition of Casting Liquidity into the Law'.

I. INTRODUCTION

In the fable *The hare and the hedgehog*, made popular by the Brothers Grimm in the 19th century, the hare dies after running the same race 74 times, confident of its sprinting prowess, but quite failing to see that the race in which it was competing was fundamentally flawed. The fable springs to mind with respect to the repeated efforts to reform European and international securities law[1] over the past 15 years. Two international Conventions, the Hague and the Geneva Securities Conventions,[2] have been adopted but not implemented and an elaborate European Clearing and Settlement Legal Certainty project[3] ended up tucked away in drawers after years of intensive work.

Since 2015, securities law has been back on the agenda, this time in the context of the European Capital Markets Union.[4] The aim is to increase liquidity in the securities lending market. This means that it should become easier to convert securities into cash, and cash into securities, at will,[5] thereby facilitating financing channels and ultimately the raising of funds for small and medium-sized enterprises. The reform of securities law, including conflict of laws and property law, has been mentioned amongst such liquidity-enhancing measures. However, the caveat that this area is 'political' and 'complex'[6] suggests that the European Commission does not intend to follow the fate of the hare and will not run the same race again. This is an understandable stance. Attempts to reform securities law are locked into the complexities of market practice, idiosyncratic approaches in areas as sensitive as insolvency and property law, and, lastly, the wrangling for market shares between financial centres in Frankfurt and Paris, on the one hand, and the City and Wall Street, on the other hand. This is why fundamental reforms are very unlikely.

This is all the more true as the market is now already moving ahead in its constant search for more efficiency and liquidity, buoyed by the idea of using blockchain technology for securities transactions, which will require a novel legal framework. It is therefore time to think about the role that should be played by

---

[1] I will use the term 'securities law' throughout this article. It refers to those rules that are relevant for holding, acquiring and disposing of securities, including the definition of the nature of securities and covering questions such as how securities are treated in insolvency. In other words, securities law comprises elements of commercial, property, corporate and insolvency law.

[2] Convention on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary ('Hague Securities Convention'), www.hcch.net/index_en.php?act=conventions.text&cid=72. UNIDROIT Convention on Substantive Rules for Intermediated Securities ('Geneva Securities Convention'); unidroit.org/english/conventions/2009intermediatedsecurities/main.htm.

[3] See, in particular, EU Clearing and Settlement Legal Certainty Group, *Solutions to barriers related to post-trading within the EU – Second Advice* (2008), http://ec.europa.eu/internal_market/financial-markets/docs/certainty/2ndadvice_final_en.pdf accessed 01.04.2016.

[4] European Commission, Green Paper – Building a Capital Markets Union, COM(2015) 63 final, available at http://ec.europa.eu/finance/consultations/2015/capital-markets-union/docs/green-paper_en.pdf, accessed 20.05.2016.

[5] For the purposes of this article I use this very basic definition of liquidity, as proposed by K Pistor, A Legal Theory of Finance (2013) 41 Journal of Comparative Economics 315-330, 316.

[6] Green Paper (n 4), 2, 6, 23, 26; Commission Staff Working Document, Initial reflections on the obstacles to the development of deep and integrated EU capital markets, SWD(2015) 13 final, 15, available at http://ec.europa.eu/transparency/regdoc/rep/10102/2015/EN/10102-2015-13-EN-F1-1-ANNEX-1.PDF, last accessed 20.05.2016.

securities law and how the legal framework for blockchain securities transactions should be designed to support legal certainty and liquidity—which, from the legislator's perspective, constitutes an immense challenge and an important opportunity at the same time.

This article traces why past developments aimed at supporting efficiency and liquidity in securities markets have been counterproductive in terms of legal certainty. Drawing on these findings, it identifies the main axioms of a future legal framework that will be legally consistent and safe and thereby support further liquidity gains, benefitting the economy and society as a whole.

Part II analyses how the interplay between market practice in search for more liquidity and the relevant substantive and conflict-of-laws rules has developed, moving from intangible loans to paper certificates and issuer registers, and from there to 'intermediated' holding, computerisation and globalisation. It shows how the law got locked into path dependencies so that today, liquidity levels are high—but at the expense of legal certainty.

Part III discusses the opaque legal nature of securities in the intermediated environment. They mainly display the characteristics of relational rights (*inter partes*), whereas legal thinking and common perception are based on an understanding of absolute rights (*erga omnes*). As this friction leads to considerable legal uncertainty, regulatory compliance of intermediaries has become the linchpin of safe securities holding, acquisition and disposition.

Part IV builds on these findings. Blockchain securities show many of the characteristics of an *erga omnes* right and are therefore, in principle, easier to capture from a legal point of view. However, blockchain securities settlement does not require intermediation, thereby fundamentally challenging the current legal and regulatory approach, which consists of focussing the law and regulation on the intermediary function. Jurisdictions will therefore need to redefine the entire legal framework. This part sets out the main axioms of such a legal framework and addresses the need for legislators to act in a timely manner in order to avoid a new spiral of path dependency and loss of legal grip on the market.

II. THREE MOVES FOR LIQUIDITY

In the early days of financing activity there were no 'securities' as such but merely mutual obligations, basically loans, between fund providers and fund receivers. Starting from this primitive state of financing, three different major developments can be identified where the economy's need for increased liquidity has shaped market practice in relation to securities and, as a consequence, the law underlying it, eventually leading to the present situation where securities are transferred electronically and used as collateral on an international scale through a global network of intermediaries. The European Commission's idea of reforming securities law with a view to facilitating financing channels in the economy is therefore by no means a novel one. Rather, it is the continuation of a development that started a long time ago.

A. Transferability, negotiation and novation

Both shares and bonds consist, in substance, of payment obligations and, most visibly in the case of shares, certain participatory rights.[7] All rights in these bundles are, by their very nature, obligations between the parties. For more than five hundred years, shares and bonds and their ancestors have been created and traded, first in Florence, later in Amsterdam and London.[8] However, businesses have also in the past faced difficulties raising as much funding as they needed, while insufficient market liquidity was also a concern.

A major limitation was the unsatisfactory transferability of these investments. Potential investors knew that it might be difficult to find secondary acquirers should they decide to divest, since transferring a bundle of mutual personal obligations to a secondary acquirer was anything but fail-safe. Long before legislators intervened to enhance transferability and thus, liquidity, the market itself developed structures and mechanisms to allow potential investors to avoid an excess of what would today be called 'due diligence'.[9] Concepts emerged capable of enhancing trading in these instruments in a legal environment in which pricing was straightforward and transparent,[10] and legally effective transfers easy to achieve.

First, potential secondary acquirers were in an uncertain position as to the content of the relevant instrument, i.e. the exact legal and economic terms of these personalised instruments were difficult to assess. The market responded by increasingly standardising the object of the transfer in legal and economic terms. Thus, it became easier for secondary acquirers to assess the position they were interested in taking. Financial instruments were issued in batches of economically and legally identical units, up to the point where securities of the same issue became not only identical as regards their content but 'fungible', i.e. no longer identifiable on an individual basis.

The second and third obstacles to transferability concern the process of transfer itself. It was difficult to ascertain whether the seller was empowered to dispose of the relevant rights and whether these were free of encumbrances. Further, assignment as a method of transfer was often unsatisfactory, in particular where only rights could be assigned but not obligations, at least not without the other party's consent.[11]

In this respect, the market developed two different concepts that are still in use today, notably transfer by delivery of a certificate, or transfer through register entries.

Civil law jurisdictions used a—very fictitious—basic legal idea to explain why delivering a certificate to the acquirer transferred a bundle of obligations: the

---

[7] Also, bonds vest certain participatory rights in a bondholder, notably to participate and vote in the bondholders meeting. See A McKnight, The Law of International Finance, OUP 2008, 531; F Nizard, Les titres négociables, Economia et Banque Revue, Paris (2003), 17-20.
[8] JS Rogers, Negotiability, Property and Identity, 12 Cardozo Law Review (1990), 470, 471-478.
[9] See Rogers, *ibid.*
[10] E Micheler, The legal nature of securities, in L Gullifer and J Payne (eds.), Intermediated Securities, Legal Problems and Practical Issues, Oxford, Hart Publishing, 2010, 145.
[11] See J Benjamin, Interests in Securities, Oxford University Press, 2000, 65-67; McKnight, n 7, s 12.9.1.

bundle of mutual obligations was coated with a property hull by 'incorporating' it in a certificate, resulting in the paper *being* the security.[12] Apart from the fact that the paper legally entitled its bearer to receive payments or to exercise participatory rights, the delivery mechanism of the certificate allowed for *bona fide* acquisition, protecting the acquirer from adverse claims.[13] Professor Rogers argues that marketability of claims did not necessarily require the benefit of good faith acquisition;[14] however, this is precisely what seems to have been the feeling at the time. In 1853, *von Savigny* described the market's need to apply the advantages of the property transfer regime, in particular the possibility of acquiring in good faith, also to obligations.[15] Other options would have been to hand, notably that of providing for the possibility of good faith acquisition of this particular type of claim immediately.[16] However, legislators chose to take the property route, according to which delivery of the certificate transfers property in the certificate and thereby transfers the relevant rights.

In England, bearer bonds are a form of documentary intangible and therefore embody the right; transfer occurs on the basis of delivery of the certificate.[17] This had already been market practice for quite some time before the English courts recognised it in the 17th century[18] and statutory law sanctioned it in the 19th century.[19] Around the same time as Savigny's proposal, in England the Bills of Exchange Act of 1882 recognised the mercantile practice of transferring obligations by endorsement (a scriptural act typically on the back of the certificate) and delivery to the acquirer.[20] This act of 'negotiation' was understood not only to achieve the transfer of the rights but also to ascertain that the *bona fide* acquirer received them unencumbered.[21]

The second option to address difficulties in the process of transfer is registered securities. The issuer's shareholder or bondholder register ensures the integrity of the issue by excluding the creation of excess rights. At the same time, it is a good means of recording encumbrances and as such it protects any future acquirer. The institute of good faith acquisition in the proper sense is therefore unnecessary.[22] In England, where registered securities are the rule, they are regarded as intangibles, or *choses* in action.[23] Historically, *choses* in action constituted a personal obligation and could therefore not be transferred by assignment without the debtor's consent,[24] and in any case assignment was only able to

---

[12] See Nizard (n 7), 294.
[13] Rogers, (n 8), 479.
[14] *Ibid*; See also CW Mooney, Property beyond negotiability, (1990) 12 Cardozo Law Review, 305, 398-99.
[15] FC von Savigny, Das Obligationenrecht als Theil des heutigen römischen Rechts, Berlin, Veit & Comp., 1853, 97.
[16] Rogers, (n 8), 479.
[17] R Goode and E McKendrick, Goode on Commercial Law, 4th ed., London (2010), 32.
[18] *Shelden v Hentley*, 2 Show. 161, cited after W Cranch, Reports of cases argued and adjudged in the Supreme Court of the United States, Washington 1804, 389-390; *Miller v Race*, Court of King's Bench (1758) 1 Burr 452 , 97 Eng. Rep. 398 (K.B. 1758), edited online version by N Szabo, http://unenumerated.blogspot.be/2006/01/from-contracts-to-money.html, last accessed 20.05.2016.
[19] Rogers, (n 8); See also JS Rogers, The Early History of the Law of Notes and Bills, Cambridge University Press, 1995, Ch 8.
[20] Benjamin, Interest in Securities (n 11), para 3.21.
[21] Benjamin, Interest in Securities (n 11), para 3.22.
[22] M Yates and G Montagu, The Law of Global Custody, 3rd ed. Tottel, Haywards Heath 2009, 20.
[23] Benjamin, (n 11) paras 2.05, 2.10.
[24] Micheler, Property in Securities – A comparative Study, Cambridge University Press, 2007, 21.

transfer the benefit, but not the burdens, of the contract.[25] The solution to this problem came with the acceptance of novation, i.e. a tripartite contract between the alienator, the acquirer and the issuer. The issuer would typically manifest its consent by changing the register. Even though the statutory basis for transfer of securities by novation dates back to 1936 and 1985, novation was already the original basis in Common law.[26]

B. Intermediation and idiosyncratic laws

Later, the industrialised world developed larger and deeper capital markets with higher trading volumes and more frequent transactions. The increasing degree of 'financialisation' necessitated more liquidity in securities markets. Transfers on the basis of negotiation of paper certificates or changes wrought to issuers' registers appeared too cumbersome, given the much higher frequency of transactions. Therefore, as the next step following improved transferability, the concept of securities intermediation through banks and brokers emerged, conceived to allow for more efficient outright transfer and encumbrance procedures. Again, the development was first driven by market practice, long before legislators sanctioned the new structures.[27] Professors *Mooney*, *Einsele, Benjamin, and Nizard* were the first, for their respective jurisdictions, to analyse the legal consequences of that change.[28]

1. Loss of the carrier, pooling and mirroring

Banks, brokers and other intermediaries connected to one another through a cascade of accounts ultimately linked to a central account ledger maintained by a central depository that also kept securities certificates, if any. As a result, in both cases of bearer and registered securities, investors received a credit entry in their securities accounts with their bank or broker. This obliterated the need to move physical security certificates (and in England: endorsement letters[29]) or change the issuer register whenever a change in ownership occurred or when securities were pledged or otherwise encumbered. The first central securities depositories for security certificates were founded in Vienna in 1878 and in Berlin in 1882, both probably modelled on the 18th century London Clearing House[30] for cheques and bank notes. However, huge chunks of securities holdings still remained in separate bank custody or in private hands. It was not until the middle of the 20th century with the advent of computerisation that this practice, now referred to as central clearing and settlement, became prevalent, and it has become the norm only

[25] Benjamin, (n 11) para 3.18.
[26] *Ibid*, para 3.06.
[27] For instance, in Germany, securities intermediation was introduced in 1882, whereas the codification of the necessary legal changes occurred in 1937, see D Einsele, Wertpapierrecht als Schuldrecht, Mohr, Tübingen (1995), 12-13.
[28] Mooney (n 14); Einsele, (n 27); Benjamin, (n 11); Nizard (n 7).
[29] Benjamin, (n 11) para 3.06.
[30] Einsele, (n 27), 12; Huang, The law and regulation of central counterparties, 44.

recently.[31] However, a number of jurisdictions, typically smaller markets or late market entrants, developed holding systems that did not entail intermediation and a cascade of accounts. In these 'transparent' systems, all investors were directly linked to a central ledger.[32]

The practice of intermediation involves three practical characteristics that have fundamental legal significance. First, it disrupts the evidencing system that had hitherto been fundamental in explaining transferability. Notably, in respect of bearer securities, the security certificate lost its practical function and ceased to change hands, being kept in a central depository or even abolished altogether.[33] Thus, bearer securities, in their practical handling, are assimilated to registered securities. As regards registered securities, issuers' books generally no longer reflect the investors' names but the names of the intermediaries first in the cascade, typically a nominee company or the largest banks and brokers in a given jurisdiction. In both cases, the carrier of the right was deprived of its function and thus became a thing of the past.

The second practical feature of the new holding pattern is that securities holdings are pooled, i.e. intermediaries hold their clients' securities through an account with another intermediary in fungible bulks of identical securities, in so-called omnibus accounts.[34] For instance, if three investors have a specific kind of security credited to their accounts with their direct intermediary, that intermediary will hold the aggregate of these securities with a second intermediary in a bulk credited to one account. This account is in the first intermediary' name, and the securities in it cannot be attributed to any specific investors.

The third practical trait with legal significance is that the 'same' securities are mirrored in different accounts with different intermediaries throughout the cascade of accounts. This means that an investor holds its securities in an account with her direct intermediary, which holds its and other clients' securities in a pooled account with a second intermediary, which holds all its clients' securities in a pooled account with a third intermediary, etc., until the chain reaches an intermediary that has an account with the central securities depository or the issuer register.[35] The length of such a 'holding chain' depends on the specific circumstances but may vary from just one intermediary to several. As a consequence, every individual security is mirrored in different pooled accounts maintained by the different intermediaries involved. The system-wide aggregate number of credit entries of a specific kind of security is therefore a multiple of the number of securities of that kind originally issued. A further complication is that securities accounts between investors and their intermediaries are structurally identical to the securities accounts that intermediaries set up between themselves. Therefore, the electronic credit entries in the accounts of investors are identical to

---

[31] See Article 3.1 Regulation 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 ('CSDR').

[32] Unidroit, Transparent Systems, Study 78 Doc 44, available at http://www.unidroit.org/english/documents/2006/study78/s-78-044-e.pdf, last accessed 18.4.2016.

[33] France was the first financial centre to dematerialise securities in 1984. See also Article 3.1 CSDR, (n 31).

[34] L Gullifer, Ownership of Securities, in L Gullifer and J Payne (eds), Intermediated Securities, (2010) Hart Publishing Oxford and Portland, 12-15; Rogers, (n 8), 485.

[35] Clearing and Settlement Legal Certainty Goup, (n 3) 30.

the electronic credit entries in the accounts of intermediaries. This obviously creates confusion as to whether these entries have a different content depending on whether they are made in favour of an investor or of an intermediary.

2. The weakened position of the securities holder

These three practical characteristics of intermediation (loss of carrier, pooling and mirroring) have significant consequences in legal terms, affecting the allocation of rights between investors and intermediaries.[36]

Notably, the specificity and identifiability of individual assets have disappeared. The fact that the securities are only identified in kind leads to the loss of an important feature of traditional property or ownership rights and of security interests on which so many holding systems were based. As exchange-listed securities are typically fungible, they are subject to rules on commingling when they are pooled. As a consequence, the quality of the right may change, for instance from a property right to proportionate ownership in the pool, or it may even become a mere claim against the intermediary.[37] The position of clients is weakened accordingly, especially in the event of the intermediary's insolvency.[38]

Further, this development placed under some strain the earlier achievement of easy and safe transferability, achieved through negotiability or good faith acquisition and the concept of the issuer register. These concepts had emerged earlier to facilitate transfer; however, with the advent of intermediation they have actually become fundamental as acquirers in this anonymous environment *de facto* have no possibility of checking who the disposer is and therefore whether it has the right to dispose of the securities. However, how could this system possibly work in an environment where both certificates and issuer registers have lost their functions, and where there are electronic account entries that all look alike but have different contents?

In other words, with the advent of intermediation, the factual elements that earlier paved the legal grounds for safe and easy acquisition were wiped out for the sake of the operational benefits of intermediation. This crack in the edifice considerably endangered what is today referred to as 'client asset protection' and, to be realistic, has not been entirely papered over so far.

3. National idiosyncrasies

In attempting to solve this problem, countries have relied on idiosyncratic approaches, thereby abandoning the homogeneity that had existed between them as long as the market was organised on the basis of paper certificates and issuer registers.

Some countries took bold steps and adapted the law to the practice (in particular the US,[39] with Canada[40] following its model), while others adapted the

[36] See Mooney (n 14), 225-28.
[37] Rogers (n 8), 485. New legislation aims at reducing commingling and the use of omnibus accounts, see CSDR (n 33), Article 38.
[38] L Gullifer (n 34), 4.
[39] See JS Rogers, Policy Perspectives on Revised U.C.C. Art. 8, (1995-96) 43 UCLA L. Rev., 1449-59.

practice to the law (in particular the Nordic countries[41] and China[42]). Some continued somehow to hover, confusingly, between these two approaches (France,[43] Germany[44]), while England[45] changed nothing at all in legal terms. What can be observed in various countries is a paradigmatic path-dependent development, where legal tradition coupled with existing market infrastructures and the vested interests of incumbent financial service providers shape not only the further development of the practice but also that of the law, regardless of efficiency, legal certainty and international compatibility. Thus, law and practice have become inextricably intertwined *per country,* where the law aligned with the operations of national central securities depositories, settlement architectures and customer account agreements.[46]

As a consequence, whereas the legal rights vested in the investor and, respectively, in a security or collateral taker, had remained comparable after the first market movements towards transferability, they now diverged significantly between jurisdictions even though the same practice was used. The legal position of investors has since become characterised as anything between a bundle of insolvency-proof claims against the intermediary ('security entitlement', US and Canada), an equitable interest either in securities or in an equitable interest in securities (England), full and unshared property in electronic bearer securities (France), full and unshared property in direct rights (Nordic countries, China), or shared or common property in a pool of chattels (Germany).[47]

The fact that national laws had become so idiosyncratic, complex and sometimes inconsistent in themselves had no significant consequences while securities markets remained mainly domestic. However, the third move towards more liquidity, notably the abolition of capital controls in many countries and the introduction of the EU single market, rendered the financial market truly international—and from that moment on, the discrepancies between the various approaches became relevant.

C. Cross-border use of securities, universal fungibility and PRIMA

Jurisdictions had barely digested, from the legal viewpoint, the emergence of intermediation when the third development began to gather pace. Since the disappearance of the Bretton Woods System in 1971, globalisation and the

---

[40] See Uniform Law Conference of Canada, Securities Transfer Act, accessible http://www.ulcc.ca/en/home/530-josetta-1-en-gb/uniform-actsa/securities-transfer-act/1124-securities-transfer-act?showall=&limitstart=, last accessed 20.05.2016.

[41] See L Afrell and K Wallin-Norman, Direct or Indirect Holdings – A Nordic Perspective, (2005) 10(NS) Uniform Law Review, 277-284.

[42] See W Liang, The Geneva Securities Convention and its Relevance for China, (2012) Law and Financial Markets Review, 287-289.

[43] See Nizard (n 7), 245-52.

[44] Einsele (n 27), 64-160.

[45] See Benjamin, Interest in Securities (n 11), 3-59; Financial Markets Law Committee, Property Interests in Investment Securities (July 2004), available http://www.fmlc.org/uploads/2/6/5/8/26584807/3e.pdf, last accessed 20.05.2016. Overview of relevant recent case law: Mr Justice Briggs, Has English Law Coped with the Lehman Collapse?, (2013) Butterworth Journal of International Banking and Financial Law, 131-132.

[46] See E Micheler, Custody chains and asset values: why crypto-securities are worth contemplating, Cambridge Law Journal (2015), 509-513.

[47] See references in n 39-45.

abolition of capital controls made available a huge asset reservoir. Markets began to use assets globally, for investment purposes, and, more importantly in the present context, to collateralise payment obligations, notably in derivative and securities financing contracts. Cross-border investment and collateralisation had, of course, always existed. However, now the share of transactions with a cross-jurisdictional element rose to 40% or more.[48]

While market practice changed towards the international use of securities, parties were unable consistently to overcome the legal obstacles associated with this practice, in particular requirements under mandatory property and insolvency laws and consequences stemming from the relevant rules of private international law. As a consequence, the market either transacted under legally uncertain conditions (thereby driving up transaction cost) or had to abstain from certain transactions altogether (provoking opportunity cost)—an argument that has now been taken up again by the Commission in the context of the Capital Markets Union.[49]

1. Lex rei sitae, lex societatis and PRIMA

Guynn[50] was the first to conceptualise the relevant shortcomings of the private international law. He argued that the place of the securities certificate (*lex rei sitae*) and the place of the incorporation of the securities issuer (*lex societatis*) as connecting factors for bearer and registered securities, respectively,[51] were unsuitable to yield a consistent result in the intermediated set-up of securities markets, let alone in the cross-jurisdictional context. Central banks, which regularly take foreign securities as collateral in exchange for liquidity they provide to commercial banks, developed a strong interest in this argument. As a consequence, legislators in Europe as well as at the Hague Conference on Private International Law rushed to address this concern by introducing a new type of conflict-of-laws rule, based on a novel connecting factor called 'place of the

---

[48] Data shows that between 5 per cent and 95 per cent of investments in the different European financial centres are allocated to cross-border securities; typically, in large financial centres like London, Frankfurt and Paris, between 30 per cent and 70 per cent are allocated to cross-border holdings. The share of cross-border *holdings* is mirrored by a correspondent percentage of cross-border *trading* activity. (Data extracted from Oxera, 'Monitoring prices, cost and volumes of trading and post-trading services', Report prepared for the European Commission, London and Brussels (2011), 73. Though the data itself relates to equity investments, the authors note, *ibid*., that they have found a positive correlation between equity and debt securities in respect of cross-border holdings.) No data is available indicating the percentage of securities *collateral* provided across borders but, going by the aforementioned figures, a significant percentage may be assumed. It is probably justified, therefore, for ease of reference, to collapse these three elements into the figure of 40 per cent of all holding, trading and collateral operations by EU market participants in one way or another imply a cross-jurisdictional element.

[49] See n 4 and n 6.

[50] RD Guynn, Modernizing Securities Ownership, Transfer and Pledging Laws, International Bar Association 1996, 5-12; see also Ooi, 'The Choice of a Choice of Law Rule', in Louise Gullifer and Jennifer Payne (eds.), Intermediated Securities. Legal Problems and Practical Issues (Oxford and Portland: Hart Publishing, 2010) 219–244.

[51] See Dicey, Morris & Collins, The Conflict of Laws, 15th ed. (2012) Vol. 2, 22-40 and 22-44.

relevant intermediary approach' or PRIMA. It was designed to facilitate the cross-jurisdictional use of securities, thereby lowering transaction and opportunity cost.[52]

2. The factual and contractual variations of PRIMA

PRIMA departs from the traditional connecting factors referring to location or incorporation. Instead, it refers to the law of the securities account to which the relevant securities are credited.[53] This law governs all securities credited to this account, whether foreign or domestic. The new approach subsumes two different sub-species: in relation to what might be termed the *Factual* PRIMA, the law of the account is the law of the place where the account is factually maintained. This subcategory is, roughly, the approach taken by the relevant EU legislation.[54] In relation to what might be termed the *Contractual* PRIMA, the law of the account is the law agreed upon to this effect by the parties. This is the approach underlying the Hague Securities Convention[55], which is also the law in Switzerland.[56]

The merits of both approaches have been hotly debated.[57] On the one hand, the Factual PRIMA may cause uncertainty because it is not always clear where an account is located where a multinational intermediary it is involved. On the other hand, the Contractual PRIMA was perceived as politically unacceptable because it would allow parties to provide collateral under English or New York law regardless of where they were located themselves, thus circumventing national mandatory property and insolvency laws. Both arguments have their merits, but what matters more in the present context is that both follow the same basic logic: the law applicable to securities disposition and acquisition is determined on an *inter partes* basis, i.e. the two-party relationship between account holder and intermediary, whereas before, *lex rei sitae* and *lex societatis* had been absolute, inflexible connecting factors.

---

[52] See Benjamin, Interest in Securities (n 11), 158-159; C Bernasconi, 'The law applicable to dispositions of securities held through indirect holding systems', Hague Conference on Private international Law, Collateral Securities Prel. Doc. 1 (November 2000). In Europe, the new rule was introduces through three sectoral Directives: Article 9(1) Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, Article 9(2) Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems; Article 24 Directive 2001/24/EC of the European Parliament and the Council of 4 April 2001 on the reorganisation and winding up of credit institutions.

[53] Ooi, (n 50), 221.

[54] See the Directives cited in n 52.

[55] Hague Securities Convention (n 2), Articles 2(1) and 4(1). The choice is restricted on the basis of a requirement that the intermediary has a qualifying establishment in the country the law of which has been chosen.

[56] Federal Intermediated Securities Act (Switzerland), Article 108c. See H Kuhn, B Graham-Siegenthaler, L Thévenoz, The Federal Intermediated Securities Act and the Hague Securities Convention, Stämpfli, Berne 2010, 1-7.

[57] Bloch, Pascale and de Vauplane, Hubert, Loi applicable et critères de localisation des titres multi-intermédiés dans la Convention de La Haye, (2005) Journal du droit international – Clunet, 3–40 ; Einsele, Dorothee, Das Haager Übereinkommen über das auf bestimmte Rechte im Zusammenhang mit zwischenverwahrten Wertpapieren anzuwendende Recht, (2003) WM – Zeitschrift für Wirtschafts- und Bankrecht, 2349–2356 ; Ooi, n 50; Sigman, Harry C. and Bernasconi, Christophe, Myths about the Hague Convention debunked, (2005) International Finance Law Review, 31–35.

3. Financial collateral and universal fungibility

This change of approach from an absolute to a relational connecting factor helped in accommodating two important market practices: the collateralisation of entire accounts and the inclusion of the value of the collateral assets in contractual insolvency set-off, often also called close-out netting. Both are extremely beneficial from an efficiency perspective and securities financing and derivatives transactions rely heavily on these techniques.

The principal efficiency gain flows from the fact that PRIMA allows entire accounts to be used as collateral, even if they contain securities from various jurisdictions. Otherwise, for instance, a portfolio comprising French, Japanese and Delaware securities could never be collateralised as a whole unless the collateral was made enforceable under the three jurisdictions, which is cumbersome and not always possible.[58] Further, PRIMA is particularly important because parties rely on the possibility to change the collateral portfolio during the course of the transaction, either to adjust its value to the changing value of the underlying obligation by adding or subtracting securities ('margining') or to exchange, during the course of the arrangement, one kind of security for another, in accordance with their business needs ('substitution').[59] This happens often on a daily basis. It would be cumbersome and legally uncertain to accommodate a change in the applicable law whenever a new kind of security is added, say, in the above example, when German securities are substituted for French ones. With PRIMA, the law applicable to the securities remains unchanged because it applies to the entire account and its—changing—content.

Secondly, parties seek to align the law governing their financial collateral with the law governing their contractual relationships, say, a derivative or securities financing transaction, which are typically concluded under English law.[60] The relevant standard documentation by default contains clauses allowing for insolvency set-off or close-out netting.[61] It is considerably easier to arrange for the value of the collateral portfolio to be included in this calculation if the applicable law can be clearly identified and—ideally—can be chosen by the parties. This is why the difference between factual and contractual PRIMA is so relevant.

Thus, the introduction of PRIMA made it possible to apply the techniques of margining, substitution and insolvency set-off, thereby contributing significantly to improved enforceability of such arrangements, allowing for quasi-universal fungibility covering securities of any kind. Their only relevant feature was, from now on, their value.

---

[58] R Goode, *et al*, Explanatory Report to the Hague Securities Convention, Martinus Nijhoff Publishers (2005), 18.

[59] See P Paech, *The Value of Insolvency Safe Harbours*, forthcoming in the Oxford Journal of Legal Studies (2016), Section 2, online version doi:10.1093/ojls/gqv041.

[60] See Global Master Repurchase Agreement, Article 17; ISDA Master Agreement, Schedule Part 4 (h).

[61] See Global Master Repurchase Agreement, Article 10; ISDA Master Agreement, Article 6.

III. ABSOLUTE AND RELATIONAL RIGHTS AND THE ROLE OF INTERMEDIARIES

The preceding part has shown how three major developments in the practice of holding and transferring securities have supported the increase of liquidity in securities markets, notably transferability, intermediation and cross-jurisdictional use of securities. Every move towards a new practice was subsequently sanctioned by legislators and the courts. However, idiosyncratic national legal approaches resulted in an uncoordinated and heterogeneous legal framework, while PRIMA introduced an *inter partes* perspective into an area of the law where, in most jurisdictions, rights are absolute, at least in principle.

Recent attempts to harmonise national laws in this regard, i.e. the Geneva Securities Convention and the EU Clearing and Settlement Legal Certainty Project, have failed.[62] At first glance, this is surprising, since the drafters concentrated on achieving a high degree of functionality and conceptual neutrality so that not only could national laws continue to apply but indeed could largely remain unchanged.[63] However, the resulting rules became so neutral in conceptual terms that they seem to suggest that any type of right, including absolute rights such as direct property, might be held in the intermediated system.[64] That, however, appears to be contrary to certain practical features of indirect holding systems which suggest that only relational rights can exist in them. Not surprisingly, as a consequence, the fundamental uncertainty whether the idea of an *erga omnes* right is at all compatible with intermediated securities holding remained and will continue to inhibit progress in terms of harmonisation.

Two types of legal framework mark clear positions in this discussion.[65] First, there is the framework epitomised by U.C.C. Article 8, where the legal solution is modelled to fit the intermediated holding system. It is built on multi-tier relational rights between the parties to securities accounts. There are no legal relationships beyond that account relationship; in particular, there are no direct rights against the issuer or any intermediaries other than an account holder's direct intermediary. The second type of legal framework is built on the contrary understanding. It is used in the Nordic countries and elsewhere. Here, investors have an identifiable, direct legal relationship with the issuer and intermediaries take no legal positions in the securitieswhatsoever. The holding system is not built on pooled accounts and does not mirror each security several times in various accounts. Instead, there is only one central ledger maintained in the central securities depository, which can be changed by banks and brokers as agents.[66] Both approaches are clear and consistent in terms of the right that an account holder receives.

A confusing position is taken by those jurisdictions that practise the former but conceptually think in terms of the latter holding system, such as France and Germany. These jurisdictions use multi-tiered holding systems as in the US

---

[62] See n 2, 3.
[63] Geneva Securities Convention (n 2), Preamble, Recital 6; EU Clearing and Settlement Legal Certainty Group (n 3), 4.3.
[64] See Geneva Securities Convention (n 2), Article 9; Clearing and Settlement Legal Certainty Group (n 3), Recommendation 4.
[65] See n 39-45 and accompanying text.
[66] See Unidroit, Study S78 – Doc 44 (n 32).

market, involving pooled accounts and mirroring each security several times throughout the system. At the same time, these jurisdictions assume the existence of an *erga omnes* right,[67] as exists under the Nordic approach. However, the indirect holding system does not provide for a set-up in which *erga omnes* positions are viable, and it is impossible for the law to impose it. Rather, the intermediated holding system is inextricably linked to a relational understanding of the rights they confer on account holders, as the following sections will show.

A. Client asset protection

Originally, paper certificates and register entries were effective carriers of the right and plausible vehicles for easy and safe acquisition and disposition.[68] However, these approaches struggled to produce consistent results as soon as the market moved on to intermediated holding. The latter boosted liquidity but came at the price of novel risks caused by intermediation, such as inadvertent or deliberate misappropriation of securities, or the creation of credit entries in client accounts that were not backed by the intermediary's own holdings. Such practices typically result in losses of client securities in the event of an intermediary's insolvency ('intermediary risk').

However, strikingly, the classification of securities as property rights has never been capable of addressing intermediary risk, even though property is generally associated with the highest possible degree of safety. The reason is that the classification as property, notably of bearer securities, was originally conceived to serve a different function, that of transferability, through vehicles such as negotiation and good faith acquisition. This transfer function was and is still needed and became even more essential in the intermediated world, as no acquirer in the anonymous environment of automated exchanges and centralised clearing and settlement would be able to verify whether the right itself or the acquisition process were free of any legal defects.[69]

However, transferability comes at the price of increased intermediary risk because it 'validates' deliberate or inadvertent misappropriation of securities and the creation of 'excess rights' by intermediaries.[70] The risk associated with this kind of non-compliance on the intermediary's side is typically borne by the original owner who would lose out if a third person acquired the right from the intermediary in good faith. This was a real risk even before modern clearing and settlement systems emerged and investors dealt with their banks or brokers on a much more personal basis: once security certificates were physically delivered into custody, the investor had no choice but to trust its custodian that it would comply with segregation requirements to keep the property identifiable, and that it would, at the same time, abstain from unauthorised dealings in the securities. If the custodian breached these obligations, the original owner was always at risk of losing the securities. Thus, with the advent of intermediation, from the perspective

[67] See Einsele (n 27), 13, Nizard (n 7), 294.
[68] Nizard (n 7), 224.
[69] Nizard (n 7), 253-257.
[70] See Nizard (n 7), 225.

of account holders, negotiability and good faith acquisition have become both a boon and a bane.

In practice, it is behavioural obligations that protect securities holdings.[71] Regulatory regimes such as the famous MiFID (EU) or CASS (UK) rules[72] impose duties on intermediaries designed to make mistakes or fraud less likely. This approach is anything but new. The first German law on indirect holding of 1896 recognised the practice of pooling and multi-tier holding and addressed the investor's resulting weak position by imposing segregation duties on the bank or broker, on threat of payment of a 3000 Deutschmark fine or up to two years' imprisonment for non-compliance.[73] However, the mere classification of securities as a property right with an *erga omnes* character could not achieve the desired level of investor protection either then or today.

B. Investor rights

A second issue is the tension between property in a security, on the one hand, and the ability to exercise the rights flowing from that security, on the other. In practice, investors are often excluded from these rights.[74] For instance, they may themselves in a situation where they are not invited to attend and vote in the annual general meeting because they are not recognised as shareholders in legal terms.[75] The root of the problem is that the connection between issuer and investor is interrupted as a consequence of the intermediated holding system, either because the legal bond between the two is broken by the holding pattern, or because operational hurdles inhibit the exercise of the rights, or both.[76]

Again, the idea of property as a specific and absolute right adds to the confusion rather than helping to sort it out, especially in cross-border situations. This is primarily because substantive securities law may attribute legal title to a person who is therefore considered a shareholder or bondholder but who is not the person taking the risk of the investment in economic terms. In the UK and the US, the holder of legal title is typically the topmost intermediary or its nominee. In France, Germany and many other jurisdictions the property is supposed to lie with the ultimate investor. In international settings, where different laws might apply to the various accounts of a holding chain, these laws, independently from each other, may even identify more than one legal owner of what is the same security in

---

[71] See Mooney, (n 14), 324-29.

[72] Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on Markets in Financial Instruments [etc.]; Financial Conduct Authority, Handbook, Client Assets, Custody Rules ('CASS6').

[73] Gesetz betreffend die Pflichten der Kaufleute bei Aufbewahrung fremder Werthpapier (1896), https://de.wikisource.org/wiki/Gesetz,_betreffend_die_Pflichten_der_Kaufleute_bei_Aufbewahrung_fremder_Werthpapiere last accessed 20.05.2016. See also Mooney, (n 14), 402-3.

[74] See J Payne, Intermediated Securities and the Right to Vote in the UK, in L Gullifer and J Payne (eds), Intermediated Securities, Hart, Oxford and Portland 2010, 187-218; Micheler (n 50).

[75] The problem exists in respect of all sorts of corporate rights in the context of distributions, reorganisation and general meetings. Dividend or coupon payments may be the only right flowing from a security that reliably reaches the investor. See, for instance, the relevant work of an ECB working group on Corporate Actions, https://www.ecb.europa.eu/paym/t2s/governance/ag/html/subcorpact/index.en.html.

[76] See Micheler (n 50), 509-513.

economic terms.[77] This sounds like a quirk of nature but in fact arises from the modern intermediated market structure supported by the introduction of PRIMA: to the extent that the question of who owns what is answered independently for each account of an intermediated holding chain there may theoretically be as many conflicting answers as there are accounts.

Even if the investor is properly identified as shareholder or bondholder, the chain of intermediaries stands between it and the issuer. As every member of the chain only knows who is next in line, communication regarding corporate rights is operationally complicated, cumbersome and costly and, therefore, often does not work.

In this set-up, again, whether or not investors are able to exercise their rights often depends on the compliance of intermediaries with behavioural obligations. This might or might not work smoothly in national systems, and it certainly does not work in the international context.[78] However, the classification of securities as a property right *per se* is of no help in this regard.

C. The Structure of Duties

Erga omnes is a term typically used to distinguish absolute from relational rights, in particular to describe the difference between property rights and obligations. The exact nature of property as an *erga omnes* right is still controversial but it generally hovers around the elements of 'right to exclude' and 'right to use'.[79] An investor in securities at present appears to have none of these; therefore, it is unlikely that securities can be classified as property.[80]

As far as the right to exclude is concerned, it refers to a duty owed by the rest of the world to the proprietor to abstain from deliberate or careless interference with the right,[81] without any special permission, in particular from converting the right, or trespassing it, or damaging it.[82] Transposing these ideas to modern securities holding, the picture seems quite straightforward at first glance: a holder of a security typically aims to exclude the whole world: the intermediaries involved in the holding from enjoying rights flowing from the securities and using them economically; the creditors of these intermediaries from accessing the securities in the event of insolvency; and other parties in general from using the securities for their own economic purposes. However, if we turn this around and ask who owes the duty not to interfere, the picture is more confusing. The focal point is the role of intermediaries alone—only they owe duties as only they have and can give access to the securities. Others can have access only through them, typically on the

---

[77] See P Paech, Market Needs as Paradigm, in PH Conac, U Segna and L Thévenoz (eds), Intermediated Securities, Cambridge University Press 2013, 36-38.

[78] See Micheler (n 32); see also the industry-wide 'Market standards for corporate action processing' which lay down very basic principles on how intermediaries should handle investor rights in a cross-border context, available at www.afme.eu/WorkArea/DownloadAsset.aspx?id=9152, accessed on 20.5.2016.

[79] See S Douglas and B McFarlane, Defining Property Rights, in J Penner and HE Smith, Philosophical Foundations of Property Law, Oxford University Press (2013) 219.

[80] See Mooney, (n 14), 412; Nizard (n 7), 305.

[81] Douglas and B McFarlane (n 79), 220.

[82] *Ibid,* 224.

basis of a court or regulatory order. Therefore, it is not entirely clear whether duties are owed by 'the whole world'.

A more fundamental point is the question of who owes these duties *to whom*. In a typical holding situation, a number of intermediaries are involved in holding the same economic asset. Only the investor's direct intermediary owes the duties *to it*.[83] Any other intermediary would typically owe duties to its own account holders, and would be unable to identify the ultimate investor. In other words, in asking who owes duties to whom, there would appear to be as many identical positions as there are accounts involved in the holding chain, in a series connection. The investor would appear not to have an *erga omnes* right against the whole world but rather a right against its direct intermediary which, in turn, is in an identical position against its own direct intermediary, and so on.

A second trait of property is that the proprietor can do with the asset whatever it pleases: use it, abandon it, do nothing at all with it, and enjoy its fruits.[84] However, the ultimate investor's right will typically only be enforceable against its direct intermediary but not against any other intermediaries involved in holding its securities: for lack of specificity and the ability to identify the ultimate investor's assets, they would all be unable to comply with its claim.[85] Consequently, the proprietor's freedom to do whatever it felt like with the security is restricted to exactly one option apart from just holding it: it can instruct its intermediary to transfer it elsewhere.

D. Conflict of laws and the broken bond between issuer and investor

In terms of conflict of laws, a similar development may be observed from the absolute to the relational perspective, contributing further to an understanding of intermediated securities as *inter partes* rights, thereby making intermediaries' duties the focal point of the legal framework.

Traditional approaches to conflict of laws in respect of securities incorporated the idea that there exists a fixed number of rights (the securities) between the issuer and its investors. For example, an issuer has issued 1m securities, and at no point in time can there ever be more or less than 1m securities. *Lex rei sitae* (for bearer securities) ensured that only the law of the *situs* of the certificate applied to proprietary questions such as acquisition and encumbrance, but no other law. *Lex societatis* (for registered securities), inversely, resulted in a situation where the location of parties and any evidencing documentation was irrelevant and only the law of the issuer applied.[86]

Therefore, conflicts between different laws as to the enforceability of rights in securities did not arise simply because the securities existed in only one place, either as a certificate or as a register entry. Thus, it was impossible for the

[83] See Benjamin, Interest in Securities (n 11), 155.

[84] Douglas and McFarlane, 'Defining Property Rights', n 79. 226.

[85] Nizard (n 7), 412; See Article 22 of the Geneva Securities Convention, which expressly excludes access to the investor's securities at the level of any intermediary other than the direct intermediary.

[86] The majority view is that *lex societatis* applies in case of registered shares, see M Ooi, Shares and other Securities in the Conflict of Laws, OUP 2003, mainly referring to the Court of Appeal decision [1996] 1 WLR 387 *Macmillan*. *Lex rei sitae* applies in case of bearer shares, where there are two scenarios: for those bearer shares in central custody that place would determine the law. For those bearer shares outside central custody, the law the jurisdiction of the location of the certificate applies.

acquisition of a security to be valid under one law but invalid under another. Both systems were closed within themselves and therefore consistently able to settle questions as to which party stood to lose and which party would win, for instance in the scenario of good faith acquisition.[87] The concept of *erga omnes* fits snugly into that environment.

By contrast, the introduction of PRIMA led to a situation in which the law applicable to a security is determined on the basis of an *inter partes* relationship. Different laws may govern the various accounts through which a security is held. This has two consequences. First, the right of the investor might be governed by one law, whereas the right in the securities certificate or register entry might be governed by another law—hence, the two economic positions are legally unconnected. Secondly, the different laws that apply to the various accounts in a holding chain may create enforceable rights that are in unresolvable conflict. For instance, the end investor may have an unencumbered property right, whereas an intermediary at a different level has validly pledged an account to its creditor that comprises the relevant security. Both aspects clearly point to the result that different assets exist in the different accounts in a securities holding chain.

The certificate and register systems guaranteed both horizontal transferability between market participants and vertical consistency between the rights originally issued by the issuer and those in the hands of investors. With the move to intermediation and PRIMA, this equilibrium shifted towards the horizontal, transactional environment,[88] in which intermediaries play the pivotal role.

IV. FROM INTERMEDIATED SECURITIES TO BLOCKCHAIN SETTLEMENT

Professor Mooney wrote in 1990 with regard to the U.C.C. that 'intermediary solvency and integrity [is] at the heart of the treatment' for improved client asset protection in intermediated systems.[89] The preceding sections show that this is still true twenty-five years on, and on a global scale. Recent insolvencies of financial intermediaries, in particular Lehman Bros., Madoff and MF Global, confirm that, while solvency and integrity requirements generally enhance investor protection and stability, they cannot protect securities holders against intermediary risk. The benefits of the current intermediated system in terms of liquidity are considerable but the system still appears flawed in terms of legal certainty and overall consistency.

However, it is not written in stone that liquidity and legal consistency are mutually exclusive. As an alternative new solution, models of un-intermediated holding, acquisition and disposition of securities have recently appeared on the agenda. Notably, the use of distributed ledger, or blockchain, technology beyond Bitcoin and other crypto-currencies is seen as a way better to consolidate the aims of liquidity and legal certainty than is currently possible in the intermediated

[87] P Paech, Intermediated Securities and Conflict of Laws, conference paper (May 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2451030, last accessed 20.05.2016.
[88] Paech, *ibid.*
[89] Mooney, (n 14), 413.

system.[90] Details of such plans are not publicly available, although it is clear that important market players invest resources in exploring the potential benefits of that idea, notably increased speed of settlement at lower cost.[91] At the moment, nobody contemplates the immediate introduction of crypto-securities for the market as a whole. Rather, the industry seems to plan using the technology for specific parts of the market and specific functions, while crypto-securities might be issued first in niche markets and probably later occur in relation to mainstream financial instruments such as shares in real economy corporations.[92] The close conceptual kinship with Bitcoin and other crypto-currencies suggests that crypto-securities may also become available to individual, even retail, investors.

With blockchain, Professor Mooney's prediction that 'innovations in technology and settlement systems might increase direct relationships between market participants and issuers and permit less reliance on intermediary control'[93] now seems to be coming true. However, that long-term shift will fundamentally change the parameters on which the current legal and regulatory framework is built, notably because the intermediary function, which currently serves as a linchpin for law and regulation, will not be part of the blockchain environment.

A. Holding and transfer of crypto-securities

Blockchain, or distributed ledger technology is able to attribute an asset to a user without the need for intermediation. 'Something' is represented by a unique piece of code and stored in an electronic vault that belongs to a market participant. The value of this piece of code can be freely determined. It could be a unit of a virtual currency, like Bitcoin, or it could be a unit in a securities issue, or something entirely unrelated to finance, like entitlements to obtain healthcare.[94] For the unit to be transferred, the transferor and the transferee connect through the Internet and the system's software effects an accrual and diminution of units in their electronic vaults.

With the lack of physical tokens, such as coins, bills or bearer certificates, there would in principle be room for error and manipulation: for instance, selling

[90] See R Ali, J Barrdear, R Clews & J Southable, 'Innovations in Payment Technologies and the Emergence of Digital Currencies' Bank of England Quarterly Bulletin 2014 Q3, available http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2499397, last accessed 20.05.2016; Wright and De Filippi, 'Decentralised Blockchain Technology and the Rise of *Lex Cryptographica*' (2015) Working paper, 11-12, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 20.05.2016; M Kalderon, F Snagg and C Harrop, 'Distributed ledgers: a future in financial services?', (2016) JIBLR 31-5, 243.

[91] GW Peters and E Panayi, 'Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, Working Paper (18.11.2015), 26-27, 30, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2692487, last accessed 15.4.2016.

[92] See, for instance, Cade Metz, SEC approves plan to issue stock via Bitcoin's blockchain (press release 15.12.2015), available at http://www.wired.com/2015/12/sec-approves-plan-to-issue-company-stock-via-the-bitcoin-blockchain/, last accessed on 20.5.2015.

[93] Mooney, (n 14), 414.

[94] See UK Government Chief Scientific Advisor, Distributed Ledger Technology:beyond block chain (January 2016), available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, last accessed 20.5.2016.

the same piece of code twice. In traditional token-less systems, such as payment systems, the problem of correct allocation of rights can only be asssured by a central entity that acts as bookkeeper for all participants. Such a central entity is not needed for assets transferred using blockchain, as a public verification process which involves many or even all participants ensures that there is no double-spending or other friction. All participants have access to this information and all accounts are regularly and automatically consolidated through the Internet.

Second-generation blockchain applications have potential beyond the mere exchange and attribution of rights. Here, the piece of code contains 'smart' elements that are able automatically to trigger performance if a specified event occurs,[95] such as the payment of dividends, or the enforcement of rights, or automatic termination, realisation of collateral or netting. Multiple smart contracts can even be bound together to form a decentralised structure that operates according to their code with no human interaction.[96]

B. Does Blockchain settlement need securities law?

Blockchain technology raises a number of regulatory and legal issues. The focus has so far been on illicit practices, such as money laundering and terrorist financing through Bitcoin.[97] There are also wider questions such as whether societies in the blockchain era will still be able to regulate commercial activity by means of the law.[98] The commercial, insolvency and securities law framework for crypto-securities and securities holding through blockchain has so far only received scant attention.[99] However, societies should consider carefully to what extent they wish to allow algorithms to replace judicial law enforcement.[100] In the transactional context, parties may be given the option to choose a conflict settlement mechanism with direct enforcement that is built into the system.[101] In the non-transactional context, the attribution of crypto-securities to market participants will need to depend on their enforceability in court. These are notably cases in which third party interests are affected, such as the interests of unsecured creditors in insolvency. And, lastly, even purportedly fail-proof mechanisms can be manipulated[102] and misused. As a consequence, a sound financial law framework for crypto-securities is indispensable.

---

[95] Peters and Panayi (n 91), 2; Wright and De Filippi (n 90), 11.
[96] Wright and De Filippi (n 98), 15.
[97] See Financial Action Task Force, Virtual currencies,: key definitions and potential AML/CFT risks (June 2014), available at http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
[98] Wright and De Filippi (n 90), especially 51-56.
[99] See JL Schroeder, 'Bitcoin and the Uniform Commercial Code' Cardozo Law Faculty Research Paper No. 458 (August 2015), available http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2649441, accessed 20.05.2016; D Quest, 'Taking security over bitcoins and other virtual currency', Corporate Rescue and Insolvency (2015), 261; P Ortonlani, 'Self-enforcing Online Dispute Resolution' (2015) Oxford Journal of Legal Studies, 1-35, doi: 10.1093/ojls/gqv036; Kalderon *et al.* (n 90), 246.
[100] See Wright and De Filippi (n 90), 51-56.
[101] See Ortolani (n 91), 15, in relation to Bitcoin-settled contracts for the sale of goods.
[102] UK Government Chief Scientific Advisor (n 94), 22; see, in relation to the insolvency of a Bitcoin Exchange, I Kaminska, Mt Gox and the mother of all short squeezes, Financial Times 20.5.2016,

Wright and *De Filippi* have shown that Nation States' ability to regulate decentralised global systems is in any case fragile and, once lost, can only be regained with brute regulatory force, entailing 'draconian' limitations to the freedom of the markets.[103] It is therefore crucial that a framework ensuring enforceability of blockchain securities settlement be developed at an early stage. If the law fails to provide consistent solutions to enforceability questions, markets will rely exclusively on operational structures and technical processes to make up for that gap. Users will push for self-regulation and the implementation of stateless mechanisms of adjudication which transcend the constraints of financial institutions and State regulation.[104] The situation of the current global intermediated system and its patchy legal framework is a reminder of how financial law can end up in such a conundrum of legal, economic and operational path dependency from which there is no easy way out. Therefore, a globally consistent framework is needed not only as a matter of legal certainty, but also in order to maintain Nation States' regulatory and legal grip on a market development that might become the infrastructure for the lifeblood of our economies.

C. The intermediated and the crypto-environment

Blockchain technology will first serve specific segments. Even though the technology has the potential to create a system entirely free of intermediation,[105] we will see a patchwork emerging with bits of the new blockchain set up side by side with the older intermediated system and probably even with the traditional paper or register-based set-up. Three scenarios can be distinguished.

1. Native crypto-securities

In a first scenario, issuers decide to issue new securities directly as blockchain instruments. I call these instruments "native crypto-securities". They would exist side by side with intermediated securities issues. The relevant legal framework would fundamentally differ and pure crypto-securities and intermediated securities cannot be confounded in legal terms.[106] However, legal uncertainty may arise in the following two scenarios where the market creates intersections between these worlds.

2. Trans-crypto-securities

In a second scenario, the issuer moves a pre-existing securities issue fully or partly from the intermediated system to the blockchain environment. I call these products "trans-crypto-securities". The situation here is quite comparable to when securities were first moved from the paper and register-based systems into the intermediated environment. The transformation needs interfaces in both operational and legal terms. Disregarding the operational side for the purpose of

---

available at http://ftalphaville.ft.com/2016/05/20/2162507/mt-gox-and-the-mother-of-all-short-squeezes/, last accessed 20.5.2016.

[103] Wright and De Filippi (n 90), 50-56.

[104] See Ortolani (n 91), 20, in relation to Bitcoin.

[105] See Wright and De Filippi (n 90), 1; Schroeder (n 99), 3.

[106] We have seen an analogous split between the register- and certificate-based market on the one hand, and the intermediated set-up, on the other hand, since the late 19th century, see above.

this paper, the legal interface will need to consist of a rule that has two functions: first to make the relevant transformed securities disappear entirely from the intermediated system; secondly, to bring the securities into circulation as crypto-securities.[107]

Both disappearance and reappearance need to be legally enforceable, including in insolvency. The possibility for rights in transformed securities to continue to be enforced in the intermediated system must be excluded. During the transformational process from paper to intermediated securities, many jurisdictions struggled in this regard, keeping the former carrier of the right alive while depriving it of its function, for example by uselessly storing security certificates in a central depository, a strategy that has considerable potential to confuse legal analysis.[108] As a consequence, there has always been a residual danger that unsecured creditors try to attach securities at the place of storage of the certificates or at the level of the issuer register, typically by means of court orders.[109]

3. Intermediated crypto-securities

In a third scenario, consortia of market players build 'crypto-enclaves' in an environment that is generally still intermediated. For instance, a group of banks may set up a settlement mechanism amongst them, using blockchain technology.[110] However, the securities settled in this enclave are issued as intermediated securities and have not undergone the transformation initiated by the issuer, as described before. Rather, participants in the settlement mechanism create 'their own' crypto-securities, which represent securities they themselves hold in the intermediated system. Here, the danger of mismatch or conflict is considerable, because the intermediated securities are what economically underpin the crypto securities. The parallel with the single most problematic trait of the current intermediated system is striking: different legal positions ultimately link to the same underlying asset, and the avoidance of conflict depends wholly on the compliance of the intermediary. If it fails to comply and becomes insolvent, the acquirers of its crypto-securities would be unprotected.

D. The point of entry for the law

Under the current intermediated approach, the PRIMA rule determines how the question of enforceability of a right in securities is connected to the law of a specific State. However, PRIMA presupposes the existence of accounts and therefore of intermediaries, which will not exist as such in the blockchain set-up. Consequently, the point of entry for the law into the world of crypto-securities is still unclear.[111]

---

[107] Switzerland has recently introduced a rule catering to the disappearance of bearer securities and their re-appearance as pure book-entry securities, see Kuhn, Graham-Siegenthaler and Thévenoz (n 56),191-211.

[108] See n 39-46 and accompanying text.

[109] See Geneva Securities Convention (n 2), Article 22.

[110] See Peters and Panayi (n **Error! Bookmark not defined.**), 27-28.

[111] See Kalderon *et al.* (n 90), 247.

1. The nature of the right and the applicable law

At first glance, the nature of the right, i.e. whether crypto-securities are claims or some kind of property, seems to be at the core of the issue of enforceability. Considering the criteria applied in the context of intermediated securities,[112] the most important communality is that both intermediated and crypto-securities represent a legal relationship between an investor and an issuer (in that, crypto-securities differ markedly from bitcoins and other virtual currencies which do not represent a claim against an issuer). The most relevant difference between intermediated and crypto-securities is that the latter are not pooled or mirrored in the system. Each crypto-security remains unique and identifiable. Further, crypto-securities directly embody the right, whereas intermediated securities in the investor's account merely relate to some root entry or certificate that is located at the top of the holding system. Lastly, the electronic vault is the single point of access to a crypto-security, and the owner of the vault is the sole key-holder. In that respect, crypto-securities come extremely close to the traditional concept of bearer securities, with the difference that the content is not set out in writing on paper but in electronic code. Therefore, it would, in principle, make sense to classify them as some kind of property and determine the applicable law on the basis of territorial considerations: the nature of the right as well as the conditions for enforceable acquisition and disposition would be determined by the law of the place of the electronic vault, or by the place of the key-holder.

However, it is doubtful whether this approach will be any help, similar to what has been described in relation to intermediated securities. The reason is that any such conceptual thinking is confined to a purely domestic legal view. The financial market is global, as is the Internet, and crypto-securities can be transferred globally across jurisdictional confines and without the need for physical infrastructures other than the Internet. However, that also means that rights in crypto-securities need to be enforceable in insolvency proceedings in basically any jurisdiction. The idiosyncratic classification of the right as property or any other type of right will not be able to provide for a legal position that will yield the desired result—enforceability—in so many jurisdictions. Therefore, other avenues will need to be explored.

A second alternative is the application of the law of the issuer, *lex societatis*, to crypto-securities. The classification of the nature of the right is irrelevant in this case, and the identification of the applicable law would be very easy in relation to each securities issue. However, this approach leads to a situation where the holding of international portfolios in a user's electronic vault requires the application of different laws to questions of acquisition, disposition and enforceability. In the intermediated environment just such a situation led to considerable legal uncertainty before PRIMA was introduced.[113] In the blockchain environment, the application of different laws to a user's portfolio would create the same uncertainty and ultimately undo much of the benefit of the new technology.

A better connecting factor for the law governing enforceability of rights is the software platform that holders of crypto-securities use. One might call that law '*lex*

[112] See above, n 79-85 and accompanying text.
[113] See above, n 51-65 and accompanying text.

systematis'. It could be determined either on the basis of a uniform choice of the users of the relevant platform or, alternatively, it could be the law of the jurisdiction of the relevant supervisor. Blockchain platforms used for securities settlement need to be regulated and supervised for systemic stability and investor protection purposes. Regulation could, in principle, allow a choice of law for the platform and its users as a whole, or, alternatively, impose the applicable law. In order to guarantee enforceability of rights in crypto-securities, it is crucial that insolvency laws around the world recognise acquisitions and dispositions effected under this law.

2. The mechanics between law and IT-based acquisition processes

As there will be different blockchain systems that operate slightly differently, it will be difficult to design a legal framework that can penetrate the technology down to the smallest detail. Rules that provide for enforceability of rights in insolvency need to be stable and cannot be adapted to frequent technological changes. Therefore, the solution may consist in creating a mechanism under which the law *refers* to the platform rules on acquisition and disposition. If the requirements of these platform rules are met, acquisitions and dispositions are enforceable. This approach is already applied to another 'black box' in the financial market, i.e. the clearinghouses.[114] As in the case of clearinghouses, enforceable acquisition and disposition of crypto-securities under the platform rules would require recognition of that specific blockchain securities platform by a public authority, notably the financial supervisor, which should also scrutinise the platform rules.[115]

However, it would need to be made clear that despite the referral to the rules of the system, compliance with these rules would still be subject to judicial review. Even though blockchain is regarded as extremely resistant to operational error or fraud, and even though some versions of blockchain systems are built in such a way as to render transactions technically irreversible,[116] the law should not be reduced to rubberstamping the outcome of an IT process. The law must retain ultimate authority over the enforceability of rights, in particular when it comes to insolvency law and other areas of mandatory law which affect third parties, as even in a near fail-safe system errors or fraud can never be entirely excluded. A strong 'good faith' rule will probably be part of the legal framework, not necessarily protecting the immediate acquirer but certainly any onwards acquirer.

In order to underline that the acquisition of crypto-securities is subject to judicial review, these rules would also need to include mechanisms allowing for the reversal of transactions.[117] Otherwise, effective judicial review could generally be countered with the argument that an erroneous or fraudulent transaction may indeed be traceable, while attempts to unwind that transaction would inevitably lead to a disruption of all transactions that have occurred subsequently on the assumption that the erroneous transaction was valid. Experience with the current intermediated system shows that the inability to reverse may be used as an

[114] See EU Settlement Finality Directive (n 50).
[115] See EU Settlement Finality Directive (n 50), Article 10.
[116] Peters and Panayi (n 91), 28.
[117] See Peters and Panayi (n 91), 29.

argument to preclude attempts to subject to review acquisition processes that have occurred in the system. However, for systemic reasons, reversal must be limited to crypto-securities still held by the immediate acquirer—it cannot extend to an onwards acquirer as this would disrupt the confidence of the entire market in the enforceability of acquisition.

V. CONCLUSION

In the wake of the markets' constant search for higher liquidity, the legal framework for securities holding, acquisition and disposition has shifted incrementally but fundamentally over time. Originally, when securities were still transferred in certificated or registered form, securities law used to be the overarching determinant defining the rights of holders and acquirers as well as their creditors. With the advent of intermediation, the legal framework became increasingly patchy and dysfunctional, and the conduct of intermediaries gained importance in respect of client asset protection. When, later on, cross-jurisdictional transactions became mainstream, the results provided by the aggregate application of different idiosyncratic laws, on the basis of the PRIMA rule, became positively confusing, and trust in international securities transactions is now mainly built on tight regulation of intermediaries and on their solvency.

The reason for this retreat of the law is that the international, IT-oriented market practice provides an ideal environment for liquidity but is fundamentally disrupted as a legal environment. This disruption stems mainly from the fact that much of the legal thinking is based on the image of specific, identifiable *erga omnes* rights, whereas the market practice is in reality hostile to that type of asset. Reform efforts have so far been unable to remove that friction because current law and practice have become heavily path-dependent and intimately linked with each other.

Now, blockchain technology is about to be introduced into the world of securities settlement, the relevant parameters will be reshuffled once again. First of all, intermediaries are in principle obsolete and are therefore not a suitable point of entry for the relevant laws and regulations. Secondly, the importance, complexity and convergence of the relevant IT-based processes will increase significantly. Thus, the function of software platforms will become the focal point of the blockchain securities environment. Thirdly, securities will again become specific, identifiable rights, very much comparable to the bearer instruments of the past.

Blockchain technology is based on an extremely fail-proof, complex technical set-up and the role of commercial law is still entirely undefined. Some might even be tempted by the idea to leave the resolution of conflicts between the different users of a software platform to the rules of that platform itself, as the intervention of State-made law might render the whole set-up less efficient from a market practice point of view. Still, a commercial law framework is indispensable. The significance of acquisitions and dispositions of securities using blockchain technology goes beyond the mere interests of acquirer and disposer as platform users. Unsecured creditors will have a crucial interest in the question of 'who owns what' in the event that either the acquirer or the disposer becomes insolvent. The answer must be given by the rules of commercial and insolvency law. Acquisitions

and dispositions effected on securities settlement platforms based on blockchain technology therefore need to be subjected to the laws of States.

Legislators would be well advised to take an interest in the law and regulation underlying blockchain securities settlement at an early stage. The picture of the current global intermediated holding system is a reminder of how disintegrated market practice and law can become. Therefore, instead of being reactive (as they have been in the past), national legislators and international bodies should now take a proactive stance and contribute to the creation of an efficient and legally safe securities settlement environment. Early and determined regulatory and legislative involvement is also important, since only a legally safe environment will appeal to the mainstream parts of the financial industry. Regulated banks, investment firms and pension funds cannot afford to move significant securities holdings into an environment that may be technically sound but which is not safe from the legal and regulatory perspective.

Considering the life-cycle of the current intermediated holding system, which first appeared in the late 19th century, the introduction of blockchain in clearing and settlement appears a once-in-several-generations chance to develop the technical environment of securities settlement in harmony with the law. In that sense, it will be the common effort of legislators, regulators and the financial industry that will be able to unlock the full efficiency and liquidity gains of blockchain technology in securities settlement.

* * *

The False Premises and Promises of Bitcoin

Brian P. Hanley

Abstract

Designed to compete with fiat currencies, bitcoin proposes it is a crypto-currency alternative. Bitcoin makes a number of false claims, including: bitcoin can be a reserve currency for banking; hoarding equals saving; and that we should believe bitcoin can expand by deflation to become a global transactional currency supply. Bitcoin's developers combine technical implementation proficiency with ignorance of currency and banking fundamentals.

JEL: E21, E22, E42, E51, G21, G29, G28

Keywords: Bitcoin, crypto-currency, cyber-currency, private currencies, alternative currencies

Correspondence: Brian P. Hanley, Butterfly Sciences, California, USA
Email: **brian.hanley@ieee.org**

The pre-publication comments of Geoffrey Gardiner and Edward Hugh on this paper are gratefully acknowledged.

1 Introduction[1]

Bitcoin is based on a paper by the pseudonymous Satoshi Nakamoto; it is a digital currency started in 2009 that creates unique, non-duplicable electronic tokens using software (dubbed mining) with an asymptotic limit of creation of 21 million tokens[1]. Every four years the number of bitcoins created is scheduled to be cut in half until 2040 when creation is supposed to go to zero. Mining is done by volunteers who operate servers running bitcoin software. The system operates by clearing transactions in a peer-to-peer decentralized system. Bitcoin provides for division of bitcoins into 10^8 parts, dubbed satoshis.

The 21 million limit on the number of tokens is intended to create scarcity, in order to support pricing of those tokens in standard currencies. At time of writing, an estimated 11-12 million bitcoin tokens have been created, and an unknown number have been lost and cannot be remade. The tokens have neither intrinsic nor price supported valuation – their price floats on exchanges against world currencies. The ability to subdivide each bitcoin into 100 million satoshis is supposed to allow for expansion of the currency.

The bitcoin ecosystem includes electronic exchanges, and an implementation of privacy, such that it is possible to use bitcoins fairly anonymously without taking unusual measures[2]. Bitcoin provides an infrastructure for transfer of its tokens, and that infrastructure is integral with bitcoin's existence. Bitcoin can be exchanged for a fluctuating amount of various national currencies, with national borders the 'highwaymen' that users wish to avoid.

Some of the earliest adopters of bitcoin as payment have been those selling illegal goods and services[3, 4]. In addition to illegal drugs, prostitution, and contract killing, bitcoin money transfer systems can be used for trans-national asymmetric warfare, although there is no direct evidence that this has occurred. In SEC v. Shavers, Mazzant

[1] This paper was submitted to a couple of mainline economics journals. It was rejected because it was considered obvious, and hence, not novel enough research. I pointed out that this created a bizarre situation, in which one could write any number of pedestrian articles on bitcoin, and get published as novel. But because the errors of thought in the conception of bitcoin were so fundamental, pointing them out could not get published. Hence, this article in *ArXiv*. I do not have endless time, and my opinion that economic thinkers have an obligation to inform other fields of study is not shared by all. But this paper has been read over by experts in the field.

ruled that bitcoins are money based on use as money and therefore investments made using bitcoin fall under regulation by the SEC[5].

Today's bitcoin community tends to be insular, with active disinterest in entering the mainstream[6]. Bitcoin has attracted popular attention and some academic interest, including technical, legal, and the rare economic scholar. The claims of this crypto-currency have virtually all been taken at face value, with little challenge to its fundamental design. However, by examining the premises of bitcoin, it becomes clear that virtually the entire enterprise is an intellectual house of cards.

The criticism herein is founded on fundamentals that have been almost completely forgone in the academic and popular record regarding bitcoin. One would hope that the errors discussed herein would be overwhelmingly obvious, but the publication record shows otherwise. Consequently, there is an "Emperor's New Clothes" cast to this critique, because bitcoin's errors are so basic.

1.1 Bitcoin representations

These premises, claims, and beliefs were derived from bitcoin FAQs[7, 8], forums, and articles[9, 10], and confirmed in conversations with proponents[2]. Most of these are direct quotes or nearly so.

1. *Bitcoin is one of the most important inventions in human history. It is the first time that the 'double spending problem' has been solved in software. Bitcoins can be put into a bank, and bitcoin loans can occur, just as with a fiat currency or gold standard currency bank.*

2. *Hoarding is another word for saving. Saving is much better than being in debt. Saving bitcoins leads to increased wealth as the bitcoin economy grows. Being in debt leads to interest payments and having less wealth.*

[2] Since initial publication, the author has discussed the contents of this paper with one of the primary cryptocurrency economists, Peter Surda. These representations were not a point of contention.

3. *Gold has the properties of being easily divisible and being of a limited supply [which] make it ideal as a currency. Bitcoins have the same properties of being easily divisible and of a limited supply.*

4. *Bitcoin proponents claim it can be expanded almost indefinitely by 'splitting' bitcoins into fractional coins. They claim that doing so functionally expands the supply of bitcoin.*

There are other representations by bitcoin proponents; however, it is not necessary to go through all of the ramifications that derive from these basic items. Seeing that list, most bankers will see serious problems on inspection, from fallacious reasoning to fundamental misconceptions.

1.2 Existing Bitcoin critiques and commentary

The European Central Bank, referencing the blog of Jon Matonis, a Forbes journalist on the board of the Bitcoin Foundation and a vocal proponent of bitcoin, voiced concerns that bitcoin has no intrinsic value and that bitcoin:

> *…fails to satisfy the 'Misean Regression Theorem', which explains that money becomes accepted not because of a government decree or social convention, but because it has its roots in a commodity expressing a certain purchasing power.* [11].

Krugman has criticized bitcoin because it incentivizes hoarding and creates deflation, but failed to note other problems[12]. Grinberg briefly touches on the possibility of bitcoin suffering a deflationary spiral, but otherwise discusses the ecosystem, technical, and legal problems; such as exchanges, potential failure of anonymity, denial of service attacks and violation of the stamp act[2]. Grinberg is an excellent reference for those interested in what bitcoin is and how it operates. Hoarding is tracked by Ron and Shamir[13], Mieklejohn, et al[14], as well as Sergio[15] without comment on its economic meaning. In addition, Mieklejohn, et al make an attempt to track circulation of bitcoins, claiming that roughly half circulate rapidly. However, since this occurs at gambling and trading sites, that activity does not represent buying and selling of goods and services.

Tyler and Moore show that patrons of bitcoin exchanges run significant risk of loss due to failure of the exchange[16].

Selgin is intrigued about a bitcoin type of crypto-currency within a fiat currency system as a way to provide a perfectly elastic currency supply that could be targeted by algorithm to various monetary schemes[17]. Selgin and Grinberg are both aware of issues inherent in an inelastic money supply. But the intractable nature of bitcoin's inelastic design is not connected by them with this issue.

A few focus on legality, providing introductory explanations of the technology of bitcoin[18, 19]. And recently:

> *California's Department of Financial Institutions has issued a cease and desist letter to the Bitcoin Foundation for "allegedly engaging in the business of money transmission without a license or proper authorization"* [20]

A precedent case for legality of bitcoin is the Liberty Dollar. However, this private currency was passed off as US currency, and contained considerably less value in silver than its face value indicated. Consequently, a significant part of that case was counterfeiting and fraud rather than stamp act violation[21]. Those features do not apply to bitcoin.

There are plenty of local or limited currencies which do not misrepresent themselves that are not prosecuted despite possibly violating the stamp act. Those currencies such as local scrip, grocery store coupons, and frequent flier miles, are redeemable in something that has a defined value in the fiat currency. Even Liberty Dollars had some intrinsic value in silver. Thus, bitcoin is unique in its pure market valuation.

Plassaras is concerned about the IMF being able to stabilize bitcoin, and states that bitcoin:

> *...poses a serious threat to the economic stability of the foreign currency exchange if it continues to grow in both value and usage. Any other digital currency that entered widespread use would pose similar problems.*[22]

This indicates that Plassaras believes that the valuation of bitcoins could reasonably be believed to be large enough that some fraction of them in the hands of one or two parties could launch an attack on the reserves of some national currency.

Some are concerned with the level of fraud and theft of bitcoins, translating into $5-$20 million in (nominal) criminal losses, together with $29 million seized by the FBI[23, 24], while others examine technical and organizational matters of bitcoin[25-28].

Jeong examines the anarchic political roots of bitcoin and cryptocurrency, as well as discussing fundamentals of the technology rather well[29]. She finds that the bitcoin cryptocurrency is part of the implementation of cypherpunk anti-government ideals along with Wikileaks, and has been identified by Julian Assange as part of the political effort of Wikileaks. She points out, correctly, that bitcoin is far less secure than commonly believed, and that bitcoin is a libertarian experiment. She identifies the irony of bitcoin's decentralized design being subsumed into dependency on a small number of exchanges and has a good discussion about bitcoin as an attempt at anarchic law. However, Jeong also fails to identify the fundamental problems of design within bitcoin I address.

Eyal and Sirer point out a serious technical vulnerability of bitcoin[30]. Bitcoin depends on the longest block-chain being the honest one. It has been understood from inception that this requires that the majority of nodes are honest. However, Eyal and Sirer describe a vulnerability that begins at 33% of computing resources. An implication is that a government (or wealthy private party) can take control of a cryptocurrency with this design (which is all cryptocurrencies now in existence) by applying superior computing resources. Even if the bitcoin algorithm is modified, it is evident that bitcoin will always be vulnerable to brute force application of sufficient computing resources to overwhelm the system.

Thus, it is apparent from examining the publication record, that bitcoin and its fundamentals are taken at face value with very few exceptions. It is also apparent that the fundamental errors in concept that will be shown date back to the origin of bitcoin, and misunderstandings about money and economics by the pseudonymous Satoshi Nakamoto[31].

2 Deconstruction of bitcoin

2.1 Bitcoin's purported capacity for expansion is not credible.

Bitcoin is currently designed to be divisible into units called satoshis that are 0.00000001 of a bitcoin[8]. That bitcoins are so divisible is supposed to mean that because 21 million bitcoins (the asymptotic limit) x 100,000,000 satoshis per bitcoin, is

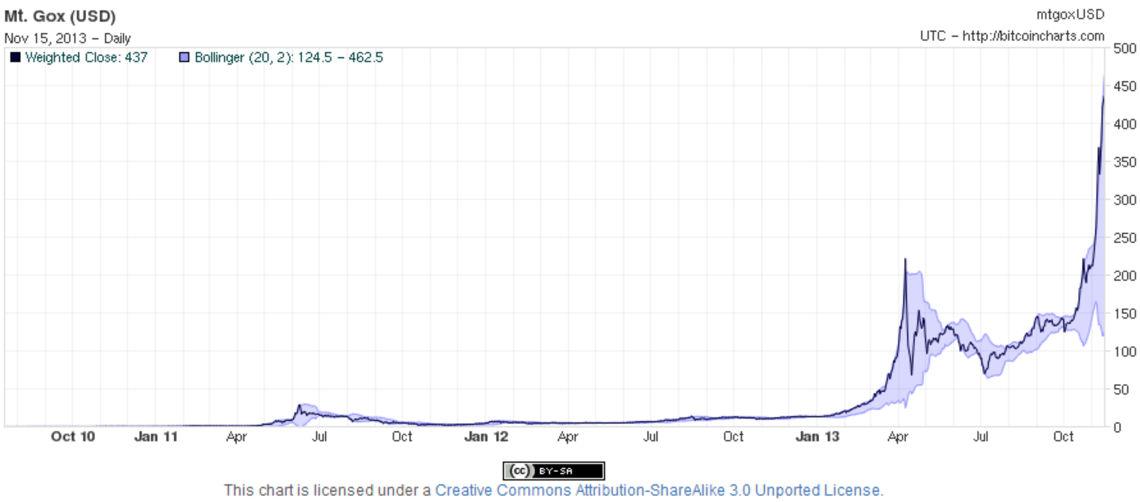
2,100,000,000,000,000 (2.1 quadrillion) that bitcoin can be a viable global currency capable of supporting virtually any degree of expansion on the scale of nations.

Bitcoin proponents may take issue with the above statement because I did not subtract 1 from 2.1 quadrillion to symbolize staying below the asymptotic limit as Karpeles has done[8]. However, for these purposes, using a limit that is larger than the real one is just as meaningful.

Additionally, there are problems with Karpeles' calculation. Subtracting 1 from 2.1 quadrillion satoshis is not correct because bitcoins are mined in integer units, not satoshis, and cataloged losses of bitcoins have almost entirely been in whole units, at least 26,609 of them[24]. (In this use of the word "loss," a bitcoin loss is a documented removal from the system of a bitcoin entity that cannot be replaced.) So the minimum theoretical number of satoshis to subtract from 2.1 quadrillion is 100 million. Based on the 26,609 documented bitcoins lost, the actual upper limit is lower by at least that many bitcoins, which is 2.66 trillion satoshis. The true upper limit may be hundreds of thousands, perhaps millions fewer whole bitcoins, because people have reported losing digital wallets, and there is no visible difference between a lost bitcoin and a hoarded bitcoin[14]. In unauthenticated reports, people lost some large wallets in the early days when they didn't think bitcoins mattered and mining them was relatively quick.

Per figure 1, at the valuation of November 15, 2013, bitcoins sell on Mt.Gox for a nominal $430 each, with a wide range. The 2012 GDP of the United Kingdom in USD was $2.44 trillion[32]. If all bitcoins were available for use in commerce, then in order to support commerce equal to the U.K. alone, each bitcoin would have to appreciate 270 times from its current peak for a total of more than 2.3 million times its earliest valuation. Not gold, silver, diamonds, oil, beanie babies, nor any other valued commodity – not even tulip bulbs[33] has achieved that. All evidence available indicates that such a wild deflationary increase in valuation would not occur.

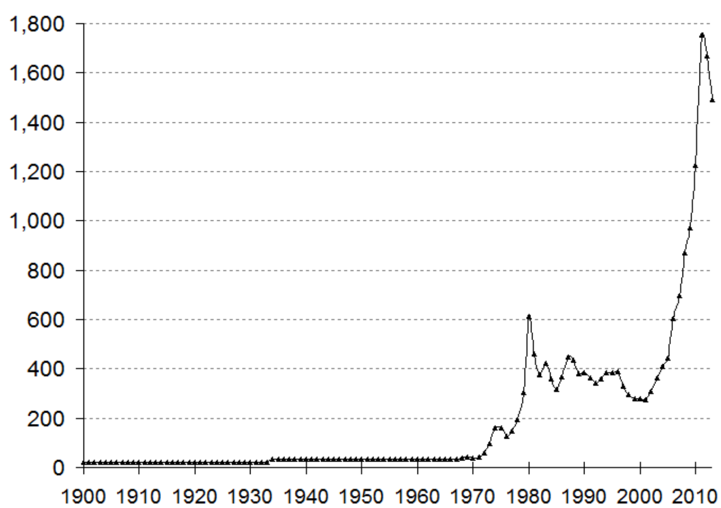
Figure 1: Bitcoin chart from Mt Gox exchange



USD exchange price from October of 2010 through July 12, 2013[34]. Periods of increasing price are deflationary periods for bitcoin. Conversely, periods of decreasing price are inflationary periods for bitcoin.

In the real world, exchange rates for precious metals have not increased in price more than one or two orders of magnitude, even over periods of time like a century as shown for gold in figure 2.

Figure 2: USD price of gold (uncorrected for inflation) over 113 years



Uncorrected for inflation, the gold price per ounce over more than a century ranged from $20.67 to $1,791.75. The high is 86.68 times the low, which is less than 2 orders of magnitude. Beanie babies at their peak sold for roughly 2 orders of magnitude more than their nominal cost when the toys were first introduced. Corrected for inflation, gold increased by just 3.19 times over a century[35].

But let us forget about that and presume, for the sake of argument, that the USD valuation of each bitcoin rose to approximately $116,600 over the next 5 years as required to match a significant economy in the world. Generating a transactional economic value close to the UK's economy spending virtually all the bitcoins in existence each year would allow us to minimize the required rise in bitcoin valuation. Starting from the valuation of $430 per bitcoin would require bitcoin's valuation to multiply by 271 times over 5 years. That would be a 109% monthly compounded interest rate.

It is impossible to imagine that commercial trade transacted in bitcoins or centi-satoshis would be robust if the valuation were increasing at such rates. No rational player would use bitcoins for spending purposes. Certainly, there are irrational participants in every economy, but it is not in the least credible to believe that virtually every player, from the wealthiest to the poorest would spend large amounts of rapidly appreciating bitcoins every year. Nor is it credible to think that a fraction of players would spend so many bitcoins that their transaction volume would approach the necessary GDP through high velocity of money through the system. Without one or the other, the level of appreciation required to allow bitcoin to support an economy of a mid-size nation would be far higher. A higher rate of appreciation means an even greater incentive to hoard, which further decreases the credibility of bitcoin supporting actual commerce.

Consequently, it is impossible to imagine that the user base for bitcoins used in commerce could enlarge enough to drive such a valuation increase. The valuation of bitcoin will always be determined by speculation, not by utility for spending. It is believable that motivated transactors will continue make use of bitcoin as an alternative for a black and grey-market payment system, although regulators and law enforcement are making that more difficult. However, what will drive speculation is the creation of an enlarged, or simply wealthier, speculator pool.

Despite a report that the Cypriot financial crisis triggered the major rise in the price of bitcoin[36] the Cypriot crisis timeline does not line up well, although it may be possible that some account holders bought bitcoins. Lacking harder evidence, the entry of the Winklevoss twins appears most likely to have driven the most recent price rise – they

claim to have acquired 1% of currently available bitcoins for their proposed ETF[20]. There is little evidence the speculator pool has enlarged much in numerical terms, but no statistics are published.

2.2 With bitcoin, reserve banking is impossible.

On a bitcoin "Myths" web page is a discussion of bitcoin and fractional reserve banking[8]. An anonymous blogger at Blogdial, cited by Matonis (who was in turn cited by the ECB) says:

> *When you have even a slight grasp of how data and computers work, and you understand that the double spending problem has been solved, your first reaction would be to gasp, as the enormity of what Bitcoin is dawns on you.*[37]

The double spending problem is the inability to transfer funds electronically without the use of a central clearinghouse that authorizes the transaction. Bitcoin has indeed solved that problem, (ignoring bitcoin's potential for takeover[30]) but a currency that *"solves the double spending problem"[10]* also ends banking as we know it.

The basis of banking is reserves[38, 39], (which reserves are now integrated around central bank money creation) and creation of new money through loans. That loan-created money is made of bookkeeping entries under the authority of banking regulators – it never exists as physical currency, and did not exist as physical currency in the heyday of precious metals[40]. Physical currency of any kind is a miniscule fraction of the money that exists.

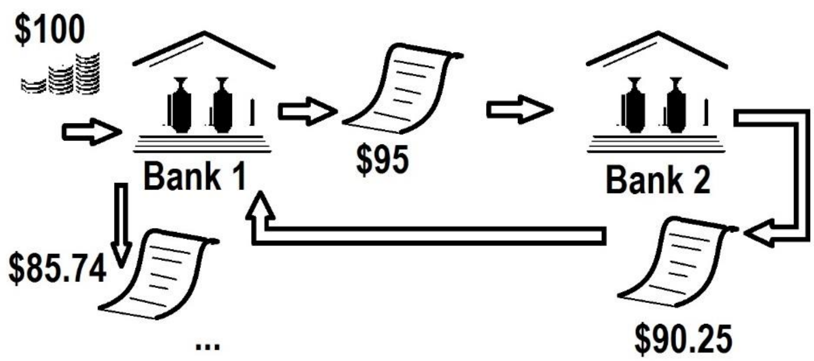
The core of the issue is that since bitcoins are unique and cannot be duplicated, bitcoin can only exist as an electronic analog kind of physical coin. Ergo no money can be created by making a loan.

In the long past, enough gold or silver was, at least in principle, required to cover reserve requirements at a bank. The need for more gold to act as the core for banking reserves was once a major matter of concern for nations. Physical currency transactions in economies began to dwindle in the 14th century with the establishment of banks in Europe[41]. Gold and silver backed currency standards came and went versus fiat money

in the 19th century. This continued until the formal ending of the gold standard in the USA in 1971, and in 2000 the formal end to the 40% backing of the Swiss Franc by gold.

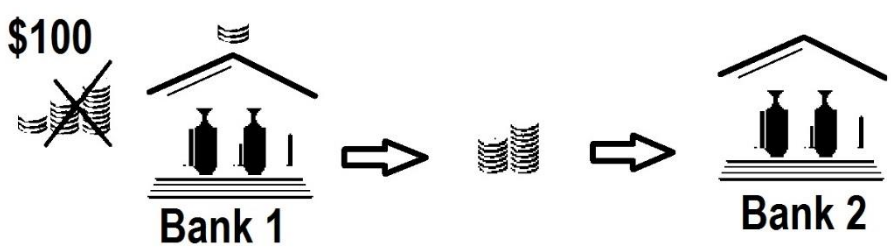
Since all bitcoins are actual coin, the amount of bitcoin is limited, and bitcoins cannot be created on demand, it is impossible for bitcoins to be used to make loans since every loan would need to be made in actual bitcoins. To clarify this let's review a classical toy banking model based on 5% gold reserves as shown in figures 3 and 4.

Figure 3: Three iterations of loans in a 5% reserve banking system.



An initial hard currency (gold) deposit is entered into the books of Bank 1. Loan paper is created of 95% of the reserve. This is "virtual money" deposited into Bank 2. Bank 2 credits this virtual money and makes a new loan, of 95% loan which is deposited into Bank 1, and that in turn is accepted on Bank 1's books, a new loan is made, etc. The result is $95 + $90.25 + $85.74 = $189.49. And that money creation can continue to the theoretical 1/r limit, where r is the reserve fraction required.

Figure 4: Physical coin system.



An initial gold deposit is placed in Bank 1 and logged into its books. Loan paper is created of 95% of the deposit. But this time the loan must be redeemed inside Bank 1 for the $95 in physical coin, and is carried out of bank 1 to deposit into Bank 2. When it is done, Bank 1 has $5 in coin and Bank 2 has $95 in coin. There is no change in the amount of money in the system, because no new money has been created by credit.

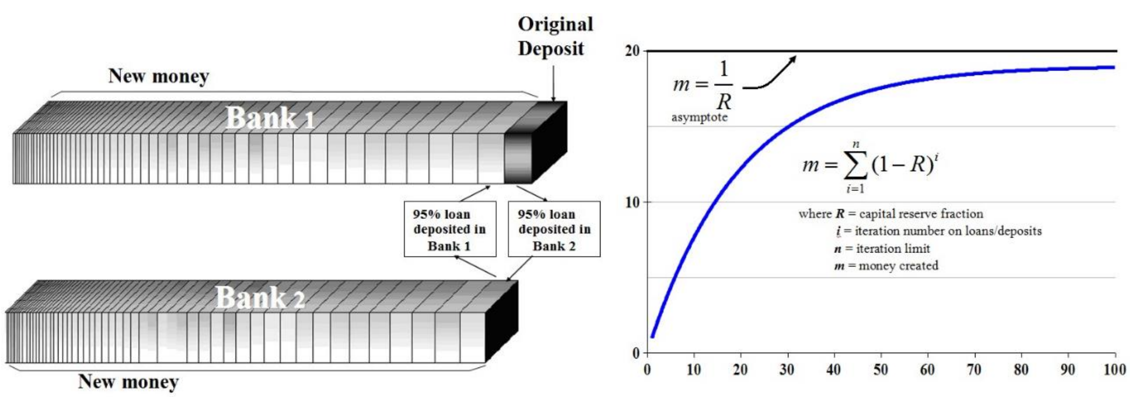
We have one of two choices here. We can allocate a new *virtual-bitcoin* to the depositor for 95% of the value of his deposit. Or, we can allocate the loan to as *virtual-bitcoin*, usable as if it were bitcoin, but not

actually real bitcoin. *Virtual-bitcoin* is precisely the kind of money that bitcoin was designed to prevent, because bitcoin's designers did not think the problem through.

Figures 3 and 4 are schematics for a classical toy banking system based on a single gold deposit. In the real world, even for a gold-backed currency, things were more complex than shown. In the time of gold-backed currency, banks had capital reserves (today tier 1 and tier 2 capital, per Basel accords[39]) and those reserves were provided by the bank's partners or stockholders, not regular depositors. The diagrams here don't differentiate this.

Capital reserves ensured bankers had "skin in the game" that they would lose if their loans went bad. Their capital regulated how much deposited money could be loaned out. But records indicate that reserves in the old system varied widely. Even as long ago as the 1840's and before, in the heyday of gold-backed currency, a bank might operate at times with practically non-existent reserves, and this was fine for the economy[40]. Thus, the difference between gold-standard and fiat money of today is less clear from evidence than it is in theory.

Figure 5: Graphical representation of banking multiplier



Each time a loan is made, it becomes a new deposit of a bank. The width of each brick in the above diagram is proportional to its size. The size of each loan declines because of reserve requirements. Equations of the banking multiplier are on the right. In practice, there are usually temporal limits to the banking multiplier, because originating a loan takes significant time. Also, loans are demand driven, which is why strategies like quantitative easing (QE) have trouble – QE is metaphorically pushing a rope.

Additionally, unlike the toy model, money from a loan would not necessarily come onto the books of a bank until it was spent. With gold and silver certificate paper notes, bank letters of credit, and bank cheques used to spend money, the net effect was similar to what is shown in figures 3, 4 and 5, but considerably messier. However, this classical toy model of banking has been good enough to educate beginning students for a long time, and is the basis for the mathematical derivation of the money multiplier asymptotic limit, so it is acceptable here.

Figures 3 and 4 make clear that creating loans based on bitcoin would require a new entity, the *virtual-bitcoin*, which would be backed by bitcoin, but not actually be bitcoin, just as gold-backed currency is backed by gold but not actually itself gold.

In this *virtual-bitcoin* scenario, bitcoin banks would keep bitcoin on reserve and redeem the *virtual-bitcoin* for real bitcoin in transfers, payments, etc. Such *virtual-bitcoins* would no longer be specific bitcoins that were deposited into an account, but instead be a *note* allowing the bearer the right to use it as if it were real bitcoin. This would correspond to a time in America many years ago when banks issued their own gold-backed currency, and the value of a bank's currency tended to vary with distance from the issuing bank.

No provision for *virtual-bitcoin* to exist in order to expand credit has been made in its design, and such ideas as paper currencies or accounting credits are anathema to the bitcoin community. The whole point of bitcoin is to force electronic transactions to only use these tokens that cannot be duplicated. To make *virtual-bitcoin* work would require a central clearinghouse to authorize the transactions, and then bitcoin would have come full circle – implementing the central clearinghouse accounting authority it was created to put an end to. Even if the objection of the bitcoin community to the idea of *virtual-bitcoin* could be overcome, it has other serious problems.

Primarily, why would a holder of a *virtual-bitcoin* note ever do anything except immediately present it for redemption in real bitcoin? We are not living in the naïve era of the Medici bankers, who could implement reserve banking without anyone being the wiser. Consequently the account holder would want to take possession of the underlying asset to prevent loss. I suppose some might prefer the *virtual-bitcoin* if enough interest

was paid. But that would be certain to end in a bank run, and the result would look very similar to a Ponzi scheme.

Physical coin (gold, silver, etc.) is heavy, bulky and inconvenient. Bitcoin is not bulky – bitcoin has indeed solved that problem gold and silver have. All the bitcoins ever made could be held in a digital ‘wallet’ on a thumb drive. So the ancient motive of depositors to have a safe place to store their inconvenient, hard to safeguard money does not exist with bitcoin – except that bitcoin can be stolen[24]. But is the problem of potential theft large enough? And an even better question is, does risk of theft go up because of depositing bitcoins, or even trading them on an exchange? Evidence indicates it does[23, 24, 42].

The Bitcoinica web site created by a teenager was allegedly the site of a massive theft of bitcoins[43]. The operator of an entity in Texas, Bitcoin Savings and Trust, (initially named First Pirate Savings & Trust) has been arrested for defrauding depositors out of their bitcoins[5].

There is an entity that calls itself a bitcoin bank named Flexcoin[44]. But it does not offer loans; its FAQ claims that it only acts to facilitate transfers. It states that it charges a 1% fee for outbound transactions. It is not, in fact, a bank, and makes that clear on its web site. It is analogous to a hawala provider[45], although what anyone would want with a central clearinghouse that charges for transactions when the bitcoin infrastructure is free is beyond my ability to explain. That Flexcoin pays some kind of interest on accounts gives rise to serious questions, since the money transfer business model requires significant charges in order to make money. With the very low fee of 1%, one has to wonder how paying interest would be conducive to making money in that business.

The Flexcoin site has no contact information, no address, no phone number, not even an email. Attempting to find a contact by domain service lookup presents an obfuscated record through an entity in Paris.

It is hard to understand why anyone would use such ‘banking’ entities when it appears more work than using the existing bitcoin decentralized infrastructure. It is even harder to understand why someone would use them when it means turning over the tokens for a currency that is not legal tender in any nation to an entity that may be difficult to identify or locate in space-time.

2.3 Hoarding is different from saving.

"Hoarding is another word for saving."

Yes, money in a mattress is saved in the general sense of the word. But no interest can be had on that money. Healthy economies have some inflation, so hoarded money is worth less when when taken out of the mattress than when it went in. In addition, money in a mattress (or cupboard, jar, etc.) is vulnerable to being stolen. There has been notable theft and fraud of bitcoins[5, 24, 42, 43, 46]. And sometimes hoards, from pirate treasure to bitcoin wallets, are lost or forgotten[47]. Articles reference bitcoin 'brain wallets' that are dependent on a memorized passphrase for retrieval. If such a person suffers death, forgetfulness, or brain damage, their bitcoins will be lost forever to all.

In the world today, banking for most citizens is like the water a fish swims in. When money is saved it is typically deposited into a bank. This makes that money available for use in the wider economy through loans, since that deposit becomes usable by the bank (or credit union) to loan, which is, of course, part of how the banking system can multiply the quantity of money in the system as shown in figure 5. Making deposited money work through loans is how banks are able to pay interest on accounts.

Bitcoins, since they cannot be used in reserve banking, (see 2.2) can only be hoarded, spent, or lost, not saved in the usual sense it is thought of in the modern world.

2.4 Loans and interest payments on loans are the engine of wealth creation.

"Being in debt leads to interest payments and having less wealth." and *"Saving is much better than being in debt."*

Debt is the acquisition of money in the present in return for a promise to pay it back in the future. Of course it is possible for consumers to get into trouble by taking on more debt than can be paid back. This has long been a problem and always will be. The source of these memes is probably in a lack of discipline regarding taking on debt, and excessively lenient consumer credit leading to the perception by the over-indebted consumer that it is debt that is taking all their money. The indebted consumer in such a case does not connect to the macro-view that the debt extended to them was new money that entered into the economy in return for goods and services.

Business uses debt as a tool to create wealth. This is fundamental to our civilization. Classically, a business borrows money to buy raw materials and tools, and then creates a value added product

that people will buy. It rarely is exactly that simple, but most businesses have a line of credit with a bank that they use to make payroll and pay other expenses during low points. A line of credit allows a business to continue operation in the sometimes very long lags between manufacturing, delivery, and getting paid. Truly, those who don't like debt don't like capitalism, because debt is another term for a loan, and loan credit is the bedrock of how capitalism works.

Businesses often extend credit, performing work and delivering a product or service before getting paid. The ordinary working person does exactly that over short periods of time by delivering a service before getting paid for it by their employer.

Wealth is goods and services in the "real economy". The financial economy is an abstract symbolic reflection of that[48]. We use money as a general medium of exchange, a store of value, etc. Creation of wealth in the real economy of goods and services requires debt. Yes, there are exceptions – some businesses operate successfully based on cash flow with no need for lines of credit; and some religious communes have operated successfully without any internal money, on the basis of mutual shared ideas, agreements, and rules for living[49]. However, even such communes used money externally, and their holdings were valued in external money of the larger society. In the social capital continuum[50], such communes are the high end. But in virtually all circumstances, debt is necessary to finance productive enterprises.

So the idea that debt leads to less wealth is backwards. In the larger economy, debt is the engine that leads to more wealth.

It is true that saving is a good thing when it supplies banks with more reserves so more loans can be made. The depositor has security for their money, receives payment that is generally above inflation, and makes capital available for loans. But the reason saving is good for society is because someone else is making use of the debt created by loans from the banking system and that creates more wealth in the real economy.

2.5 Saving bitcoins leads to increased (*personal*) wealth – but only when there is bitcoin deflation.

"~~Saving~~ [Hoarding] bitcoins leads to increased wealth as the bitcoin economy grows." This idea appears on its face to be self-evident. But in reality it is self-contradictory.

When bitcoins increase in value, they are deflating. Deflation is a characteristic of economic depression, not a growing economy, and it is the bitcoin economy that is supposed to grow. Deflation creates a liquidity trap for debtors [51] because their real interest rate is equal to the deflation rate times the formal interest rate of their loan.

Thus, if a month's deflation increases the valuation of a currency by 1%, and the monthly compounded interest rate is 0.5% (a yearly yield of 6.1%) then the true effective interest rate is 1.505%[3]. This looks small, but when compounded monthly, the yearly yield is 19.6%[4] per year, which is 13.5% above the formal 6.1% per year yield.

This can put debtors into a 'cash crunch' because they no longer can afford to pay their bills and service the loan. That means the bank will foreclose on the collateral for the loan, which is usually the assets of the business or individual. If it is a business, then the employees lose their jobs, suppliers don't get paid, and that business stops producing wealth in the real economy. Employees that lose their jobs can no longer afford to pay their bills and service their loans, and so other loans go under. That is the cycle that the Federal Reserve has been fighting with quantitative easing.

In addition, when money increases in value relative to goods and services of the real economy, then hoarding of money becomes a winning strategy. The higher the rate of increase in the value of money, the more effective is the hoarding (or miser) strategy. This may appear trivial to naive readers who might think that if the money is deposited into a bank that the bank can pay some level of interest, so it's all fine. But banks make their money on the spread between what they pay for money and what they receive in net return on loans. When the currency is increasing in value (deflating) what a bank is able to pay in interest can become less than zero. Less then zero is not typically an attractive interest rate to depositors.

When loans go bad in larger fractions than normal, the bank doesn't make as much money as it did and there are fewer creditworthy borrowers to pay the bank for loans. So depositors can't make much, and they may not be able to get their money back because the bank has too many bad loans. If depositors have amounts larger than the bank has in deposit insurance, then depositors can get caught in the downdraft. That sort of thing is what motivated people in the great depression to save their money in a mattress so they wouldn't lose it, and that crisis resulted in the FDIC.

As already seen, money that is hoarded is not productive money in the real economy because it is not invested and can't be made the basis for loans. Consequently, the economy has to suffer. Looking at the chart in figure 1, one can see a bubble occurred more than once that drove up the price of bitcoin, deflating the currency. Analyses of the bitcoin blockchain record show that hoarding is a serious issue[13-15].

---

[3] $1.01 \times 1.005 = 1.01505$

[4] $1.01505^{12} = 1.196$, or 19.6% interest.

Bitcoin proponents have answered criticisms about deflation with declarations that lack evidence. For instance:

> *"As deflationary forces may apply, economic factors such as hoarding are offset by human factors that may lessen the chances that a Deflationary spiral will occur."[8]*

In a time of rising prices, sellers would be interested in selling their bitcoins at the highest price they can. Conversely, buyers of bitcoins are less interested in taking them at the highest valuation because they may not be able to exchange their bitcoins for a less volatile currency before the bitcoin price drops, which tends to result in hoarding. This problem applies also to merchants. On highly volatile days, goods or services sold for payment in bitcoin could lose significant value in standard currency before exchanging them. So absent rigorous identification of what those claimed human factors are, together with a sensible model of human behavior during deflation, declarations such as the above are not credible.

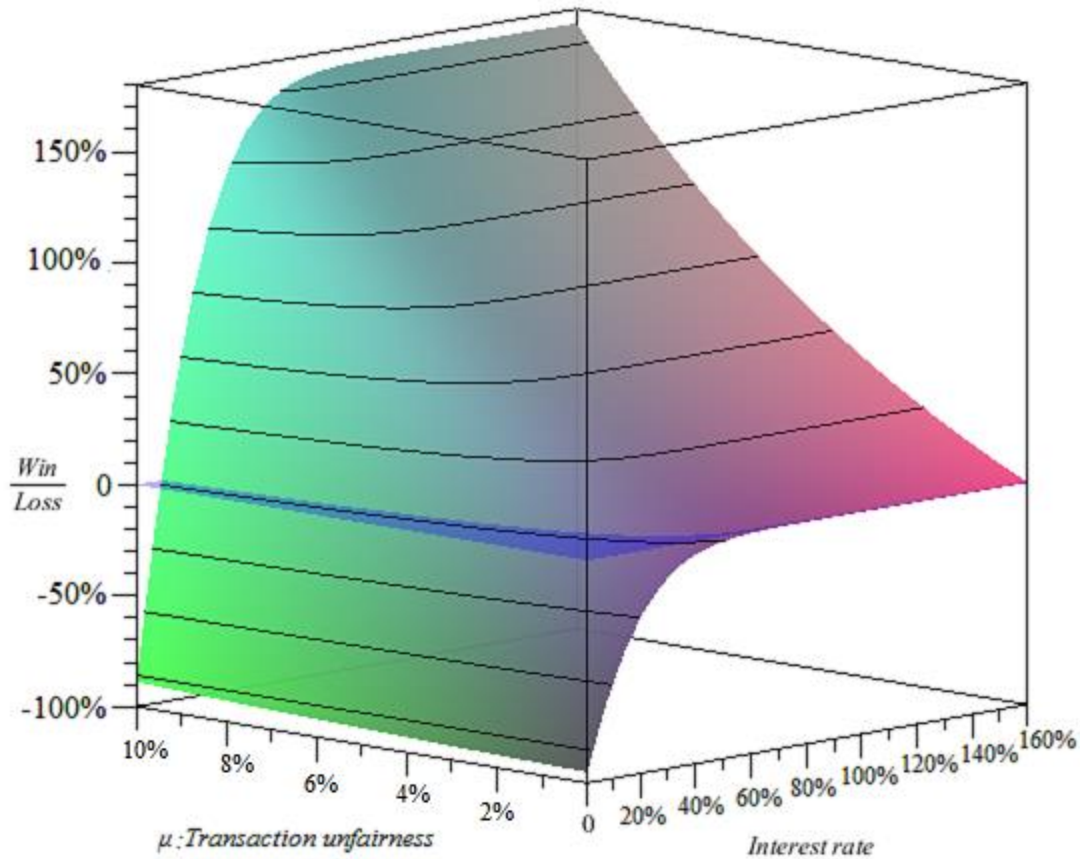
Hoarding of a medium of exchange results in deflation (rising valuation) and a shrinking economy unless there are other currencies that predominate. In the case of bitcoin, those other currencies are the various fiat currencies of the world.

2.6 A bitcoin financial system is a losing zero-sum game for investors.

A system where the amount of money is fixed is a zero-sum game – for every winner, there must be a loser, because new money is not created that allows interest or investment return payouts. Bitcoin is designed to be a zero-sum game, and long before bitcoin creation is formally set to zero, the accidental loss of bitcoin wallets will match or surpass the creation rate. It is quite possible that this point has already been passed, but there is no way to monitor it because most bitcoins are hoarded, not used in commerce, and due to the distributed design, there is no visible difference between a hoarded bitcoin and a bitcoin that has been lost forever. Consequently, bitcoin is worse than a zero-sum game. It is a pulse game in which the bitcoin resource is injected and then slowly drawn down.

Without banking to make credit available, or without the ability to expand the money supply in concert with economic activity, interest payments in a zero-sum game can only cannibalize the money supply to pay winners. This forces a loss for every gain[52].

Figure 6: Interest rate, unfairness and investor return



If the scales are unfairly tilted in favour of the investor class, the investor class can net a positive return, up to the limit of the money in the game. Within the investor class, probability dictates that some will be winners and others losers regardless of the interest rate, but the class as a whole will see these outcomes. Many will be surprised that to break even with a 5% advantage, the investor class requires an approximate 17% simple interest rate. [52]

A rational player rigs the game, or else charges outrageous amounts of interest/investment return. Even in a zero-sum game in which nobody understands, the system will evolve players who play the game according to winner's rules. We still have rules handed down from ancient times against usury and historical records of very high norms for interest rates in the past that indicate that ancient money-lenders evolved to conform to high interest rates.

This indicates that whatever bitcoin economy exists is dependent on the non-bitcoin economy for growth, because lending bitcoins in a pure bitcoin economy should have serious issues due to limitations on creation of money.

3 Conclusion

After having bitcoin explained to him, the most experienced banker I know said:

> *[bitcoin is]…a very clever practical joke by someone who is having enormous fun exposing in the most sophisticated way imaginable the naivety of clever mathematicians, economists and/or rich speculators. ... or ... The cleverest con trick ever conceived, and probably one of the most rewarding.[53]*

My opinion is that bitcoin is most likely an accident born out of ignorance with some pecuniary interest thrown in. It should be obvious that even though bitcoin was created with built-in scarcity, every bitcoin in existence is itself newly created money. This is another irony of bitcoin – while bitcoin proponents decry the ability of governments to manufacture money, bitcoin is an entirely manufactured currency, which proponents intend to value in fiat currencies in order to profit. It should also be obvious that certain proponents have positioned themselves to make money by running exchanges and accumulating bitcoins. Those exchanges have no transparency, and the arms of regulators are only in the nascent phases of reaching bitcoin transactors. Bitcoin exchanges are positioned to trade on their own accounts in addition to charging fees.

An ECB publication states that bitcoin's theoretical roots are in Austrian economics[11]. Bitcoin corresponds with Austrian economic ideas in that bitcoin was intended to provide a monetary alternative that is beyond the reach of governments to regulate. Bitcoin has correspondence with libertarian ideas, which have some relationship with Austrian ideas. In the USA, my experience is that bitcoin proponents appear to have obtained their theory from science-fiction, radical libertarian popular literature, anti-government/anti-tax activism, and often from nothing that is apparent except their own thoughts[5].

[5] I certainly don't wish to discourage anyone from independent thinking. I merely wish to point out that there is a body of knowledge already developed which can improve understanding of economics, money and banking.

Bitcoin was developed by a motivated group of technologists who dreamed of creating a new currency that would cause fiat currencies to wither away. They believed that they had to do it with a distributed architecture that avoided a central clearing house in order to escape governmental control, an architecture that required that the tokens could not be duplicated. They wanted to do this because they believe that fiat currencies are the root of financial evil. They wanted to apply the Silicon Valley idea of 'disruptive technology' to the world economy.

There are precedents in history for successful disruption of finance. Hawala[54] type money transfer systems were disruptive. This invention of letters backed by the contents of a vault defended by a powerful clan was the first step toward changing the world. Those were hawala type practitioners, entities that took a commission in return for writing a letter to someone in another location so that the party using the service would not be required to move the material across regions where it could be stolen. That system established transactional convenience. Hawala was disruptive to those who made their living by robbery, and it enabled trade. But it wasn't yet banking.

The invention of banking was massively disruptive. It took power from royal families, making them beholden to bankers. The world we take for granted today in which a middle class life is presumed normal for most, a world where markers of health and wealth have vastly improved worldwide[55] could not exist without the banking revolution that put money creation into private hands. Banking made it possible to have competence win out over political favors to allocate capital. Banking created a revolution that made it feasible to extend credit at low rates of interest without necessarily having to rig the game – because the money system was no longer a zero-sum game. Very slowly, that revolution pushed the availability of credit downscale until today we take it for granted that virtually anyone in the developed world can get credit, and microloans are spreading all over the world. Ironically, it is the very ease of availability of that credit to consumers that fuels naive ideas of bitcoin proponents, such as that debt destroys wealth.

There may be a useful place for alternative forms of electronic money. However, an improvement requires study of money, financial institutions, finance history, and understanding of how and why our system works as it does today. At best, bitcoin is an unintentional throwback to pre-medieval finance.

As a currency to take over the world economy, or even a tiny part of it, bitcoin is not credible. Nor is there evidence in the history of commodity or currency valuations to suggest that the increase in price of bitcoins necessary to fulfill the dreams of proponents could reasonably be expected to happen. Similarly, there is no reason to think that a currency backed by nothing – a pure confidence currency – could overcome its hoarding and speculation problems and actually become an instrument used significantly for commerce.

I think that it would be helpful to put thought into developing systems that: A.) made credit more available to wealth-creating enterprises in the real economy; B.) improved evaluation of business ideas and startup teams so that loans could replace venture capital for many enterprises; and C.) improved allocation of capital within sectors so that capital does not repeatedly over-invest in the latest 'hot sector' thereby guaranteeing a lower average aggregate rate of return. In my view, those would be productive goals to work toward. Creation of a dysfunctional speculation vehicle is not a positive direction.

4 Afterword – Thoughts on how to disrupt finance in a positive way

This paper was primarily written in hopes that those involved with bitcoin can be reached and shown certain errors. The bitcoin community comes from an industrial sector that pays homage to disruption and Schumpeterian entrepreneurial spirit. What that community needs to understand is that banking is the original "disruptive technology". Banking changed the world. If you look around you, most of what you look at, from the desks, tables, computers and walls, to the clothes on your back, exists because banking made it possible. Banking is still evolving. In this afterword, I will provide my thoughts on how that spirit can be applied to finance, but in a positive way.

Within enterprise investment, I have observed first-hand that the people who make decisions to invest or loan money are often as ignorant of the area they invest in as bitcoin developers are of banking. Likewise, those who understand a technology are often equally ignorant of finance and business organization. These are problems that need to be solved somehow in order to serve the public good.

Perhaps a public market for underwriting of credit default swaps (CDS's) on real-goods/services enterprise investment could help to crowd-source investment decision-making. The software industry likes to think of itself as the originators of crowdsourcing, but stock and bond markets are the original crowdsourced decisions. When looking at what AIG did wrong, it was not writing CDS contracts, per se, that was the problem, it was a risk model that didn't coincide with reality. Perhaps that invalid model was deliberate, since the public would be on the hook to pay, and executives made bonuses while the music played, but that is speculation, and a separate problem.

In my opinion, CDS contracts are inappropriate for relatively fixed assets like real estate, because new value creation is almost entirely in the initial development. The temptation to abuse CDS contracts is great. However, they could be a good thing for enterprises that are creating real value. Using CDS contracts with the current Federal Reserve rules allows for very high growth – if it is warranted[56]. It was precisely that explosive growth that generated the housing bubble. In itself, rapid money creation isn't wrong. However, it needs to reflect something real, without overheating.

It used to be that an investment bank was a special kind of entity that was allowed to risk the money of its participants in investments. This made a lot of sense. If you can invest your money as a bank, then you can improve your returns.

Over time, investment banks like Goldman Sachs got more and more freedom, until they are no longer anything like what was originally intended. I think that we need something like an investment bank – perhaps we could call it a "Venture Bank" and allow it special privileges similar to the old rules for investment banks, but only if it will invest directly in real enterprises directly producing value.

Another idea that might help would be to create a banking infrastructure entity that could allow individuals or groups to manage their own money as an investment bank. Some floor of assets is needed, but aside from that? Why not give those people access to the Central Banks, just like the majors have? In this internet age, it could be done. It would allow people to learn how banks really work, and understand better where money comes from. It could, perhaps, even the playing field, vis-à-vis the giant banks. And it just might be possible to implement within the political system we have.

All of those readers who are newly minted millionaires and billionaires, think about it. Why shouldn't you be able to maximize the utility of your money by operating your investments as a bank? Back in the 19th Century, bankers like J.P. Morgan rocked the world. Morgan backed Tesla (the man, not the car company) and much else. Bankers with vision built things. But the gold standard meant the world banking system would periodically bump up against the limits of money creation. (Look at figure 5, right. When you are on the steep side of that curve, money is easy. The closer it gets to the ceiling, the tighter money gets.)

The gold standard problem is what the Federal Reserve/Central Bank system fixed. Yes, I am aware that many involved with bitcoin believe that "The Fed" is the root of all evils, etc. I am all too aware of the Tea Party movement's Alice-In-Wonderland views. "The Fed" and Central Banking is not "the problem". But virtually everything else is. The Fed and Central Banks around the world are the best functioning parts of our finance system today.

I have also seen first-hand that venture capitalists are lemmings. This isn't a new observation. I got my first invitation to lecture at the Leavey School MBA program after an argument with a professor about this issue. You see, what the lemming method accomplishes is to guarantee lower rates of return for venture capital. If a sector is over-invested, then it's obvious that many are going to fail – not because of incompetence – it's pure numbers. However, the lemming methodology is the inevitable outcome of the finance sector's inability to evaluate well what they are investing in. What else can they do? Certainly, deciding when a sector is over-invested, or even what the boundaries of a sector are, is a fuzzy problem – it's art, not science. But there are points when everybody with their hands in knows that there are too many.

So, to those interested in creative disruption, I would recommend:

- Investment/venture banking for the masses, or something like it.
- Venture banking to bring back what investment banks once were.
- Open-outcry exchange for all CDS contracts.
- Attempting to develop CDS type contracts on investments in startup and existing enterprises.

- Improving the connection between startup tech/ideas, business organization and investment.

That could be disruptive in a positive way.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin*, 2009. http://bitcoin.org/bitcoin.pdf

[2] R. Grinberg, "Bitcoin: An Innovative Alternative Digital Currency," *Hastings Science & Technology Law Journal*, vol. 4, pp. 160-208, Nov 11 2011. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857

[3] N. Anderson and C. Farivar. (2013, How the feds took down the Dread Pirate Roberts. *Ars Technica*. Available: http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/

[4] P. Bharara, G. Venizelos, B. Crowell, and T. Weirauch, "Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of “Silk Road” Website ", ed: Federal Bureau of Investigation, 2013. http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website

[5] "SECURITIES AND EXCHANGE COMMISSION V. TRENDON T. SHAVERS and BITCOIN SAVINGS AND TRUST ", ed: US District Court, Eastern District of Texas, Sherman Division, 2013, pp. Document 23, PageID #566. http://ia800904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf

[6] (2012) (Accessed: July 12). D. Stuckey. *Does the New Bitcoin Bank Defeat the Purpose of Bitcoin?* Available: http://motherboard.vice.com/blog/bitcoin-bankers-want-to-steal-the-show

[7] (2010) (Accessed: July 11). Anonymous. *Understanding Digital Currency*. Available: https://docs.google.com/document/d/1azCQj6KisPv6E-Ez1B2oLuGMfNowFkvDuH4PXa4pzLM/edit

[8] (2013) (Accessed). M. Karpeles. *Myths*. Available: https://en.bitcoin.it/wiki/Myths

[9] M. E. Peck. (2012), Bitcoin: The Cryptoanarchists’ Answer to Cash. *IEEE Spectrum*. Available: http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/

[10] J. Matonis, "Why Are Libertarians Against Bitcoin?," *The Monetary Future*, Jun 16 2011. http://themonetaryfuture.blogspot.com/2011/06/why-are-libertarians-against-bitcoin.html

[11] ECB, "Virtual Currency Schemes," *European Central Bank*, Oct 2012. http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[12] P. Krugman. (2011, Golden Cyberfetters. *The New York Times*. Available: http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/?_r=0

[13] D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," *IACR*, 2012. http://eprint.iacr.org/2012/584.pdf
[14] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," *Proceedings of the 2013 conference on Internet measurement conference* vol. IMC '13, pp. 127-140, 2013. http://dl.acm.org/citation.cfm?id=2504747
[15] Sergio, "The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius," in *BITSLOG*, ed. Wordpress, 2013. http://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/
[16] T. Moore and N. Christin, "Beware the middleman: Empirical analysis of Bitcoin-exchange risk," in *Financial Cryptography - Lecture Notes in Computer Science*. vol. 7859, A.-R. Sadeghi, Ed., ed: Springer, 2013, pp. 25-33.
[17] G. Selgin, "Synthetic Commodity Money," *University of Georgia Economics* Apr 10 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118
[18] R. Bollen, "The Legal Status of Online Currencies: Are Bitcoins the Future? ," *Journal of Banking and Finance Law and Practice*, vol. 2013, May 1 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285247
[19] N. M. Kaplanov, "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation," *Temple University Legal Studies Research Paper*, Mar 31 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203
[20] (2013) (Accessed: Aug 15). N. Mattise. *California sends cease and desist letter to Bitcoin Foundation*. Available: http://www.wired.co.uk/news/archive/2013-06/24/bitcoin-cease-desist-california
[21] (2010) (Accessed: Jul 11). A. J. Kirby. *The strange case of the Liberty Dollar*. Available: http://www.silvermonthly.com/the-strange-case-of-the-liberty-dollar/
[22] N. Plassaras, "Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF " *Chicago Journal of International Law*, Apr 22 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2248419
[23] J. Edwards. (2013, Nov 17) If Bitcoin Is So Secure, Why Have There Been Dozens of Bitcoin Bank Robberies And Millions In Losses? *Business Insider*. Available: http://www.businessinsider.com/the-history-of-bitcoin-theft-2013-11
[24] (2012) (Accessed: Aug 15). Dree12. *List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses*. Available: https://bitcointalk.org/index.php?topic=83794.0
[25] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. Böhme, "Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency," *Workshop on the Economics of Information Security WEIS 2012, Berlin, Germany*, Apr 18 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2041492
[26] M. Elias, "Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy " Oct 3 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1937769
[27] W. J. Luther and J. Olson, "Bitcoin is Memory," *Kenyon College*, Jun 9 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2275730
[28] R. Teigland, Z. Yetis, and T. O. Larsson, "Breaking Out of the Bank in Europe - Exploring Collective Emergent Institutional Entrepreneurship

Through Bitcoin " *Stockholm School of Economics*, May 12 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2263707

[29] S. Jeong. (2013, The Bitcoin Protocol as Law, and the Politics of a Stateless Currency. *Constitutional Law of Money Seminar, Harvard Law School*. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2294124

[30] I. Eyal and E. G. Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," *Arxiv*, 2013. http://arxiv.org/abs/1311.0243

[31] S. Nakamoto, "Bitcoin open source implementation of P2P currency.," *P2P Foundation*, 2009. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562

[32] IMF, "World Economic Outlook Database - Report for Selected Countries and Subjects " International Monetary Fund, Washington, DCApr 2013

[33] C. Mackay, *Extraordinary Popular Delusions and the Madness of Crowds* 1841. http://www.gutenberg.org/ebooks/24518

[34] (2013) (Accessed: Nov). *Bitcoin Charts - Mt Gox*. Available: http://bitcoincharts.com/charts/mtgoxUSD

[35] (2013) (Accessed: Nov). M. Friedman. *The Inflation Calculator*. Available: http://www.westegg.com/inflation/

[36] P. Delevett, "Bitcoin gets big bets from Silicon Valley," in *San Jose Mercury News*, ed. San Jose: San Jose Mercury News, 2013. http://www.mercurynews.com/business/ci_23726452/bitcoin-gets-big-bets-from-silicon-valley

[37] Blogdial, "Refuting the attacks on Bitcoin's design," in *Blogdial* vol. 2013, ed, 2011. http://irdial.com/blogdial/?p=3064

[38] FRS, "Commercial Bank Examination Manual," F. R. System, Ed., ed. Washington, DC: Division of Banking Supervision and Regulation, Board of Governors of the Federal Reserve System, 2000, p. 1068. http://www.federalreserve.gov/boarddocs/supmanual/cbem/0005cbem.pdf

[39] BIS, "Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems," ed. Basel, Switzerland: Bank for International Settlements, 2010.

[40] T. Tooke, *An Inquiry into the Currency Principle, the Connection of the Currency with Prices, and the Expediency of a Separation of Issue from Banking*. London: Longman, Brown, Green and Longmans, Paternoster-Row, 1844. http://www.efm.bris.ac.uk/het/tooke/currency.htm

[41] N. F. Hoggson, *Banking through the ages*. New York Dodd, Mead & Company, 1926. http://openlibrary.org/books/OL6688843M/Banking_through_the_ages

[42] (2013) (Accessed: Nov 15). L. Mathews. *$4.1 million worth of Bitcoins goes missing as Chinese exchange GBL disappears*. Available: http://www.geek.com/news/4-1-million-worth-of-bitcoins-goes-missing-as-chinese-exchange-gbl-disappears-1576967/

[43] "BRIAN CARTMELL et al VS. BITCOINICA LP, ALSO KNOWN AS BITCOINICA et al," in *Judge Marla Miller*, ed: Superior Court of San Francisco, 2013.

[44] (2013) (Accessed: Jun). *Flexcoin bank*. Available: http://www.flexcoin.com/

[45] A. A. Shah, "The international regulation of Informal Value Transfer Systems," *Utrecht Law Review*, vol. 3, pp. 193-218, Dec 2007. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1083689

[46] C. Cumming, "SEC Says Ponzi Scheme Defrauded Investors of Their Bitcoins," *Bank Technology News*, Jul 23 2013. http://www.americanbanker.com/issues/178_141/sec-says-ponzi-scheme-defrauded-investors-of-their-bitcoins-1060813-1.html

[47] V. Harrison. (2013, Nov 29) Bitcoin worth $9M buried in garbage dump. *CNN Money*. Available: http://money.cnn.com/2013/11/29/news/bitcoin-haul-landfill/

[48] R. G. Ibbotson and P. Chen, "Stock Market Returns in the Long Run: Participating in the Real Economy - Yale ICF Working Paper No. 00-44," *Yale International Center for Finance,* vol. 00-44, 2002. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=274150

[49] M. Holloway, *Utopian Communities in America 1680-1880 (Formerly titled "Heavens On Earth")*. Mineola, New York: Dover Publications, 2011.

[50] F. Sabatini, "Social Capital as Social Networks. A New Framework for Measurement," *Sapienza University of Rome - Department of Economics and Law,* 2005. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=755065

[51] A. Orphanides, "Monetary Policy in Deflation: The Liquidity Trap in History and Practice - FEDS Working Paper No. 2004-01 " *Board of Governors of the Federal Reserve System,* 2004. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=512962

[52] B. P. Hanley, "A zero-sum monetary system, interest rates, and implications.," *Arxiv,* 2015

[53] G. Gardiner, "What bitcoin is," B. Hanley, Ed., ed. email, 2013.

[54] N. Passas, "Hawala and Other Informal Value Transfer Systems: How to Regulate Them?," *Risk Management: An International Journal,* vol. 5, pp. 49-59, 2003. http://www.jstor.org/stable/3867818

[55] (2012) (Accessed: Aug 17, 2012). H. Rosling. *Gapminder*. Available: http://www.gapminder.org/ - Gapminder World/Health and Wealth of Nations

[56] B. P. Hanley, "Release of the Kraken: A Novel Money Multiplier Equation's Debut in 21st Century Banking," *Economics e-Journal,* vol. 2012, 2012 http://www.economics-ejournal.org/economics/journalarticles/2012-3

THE RISKS OF BITCOIN USE

Mircea PLOTEANU*[1]*, licentiate in economic sciences,
Academy of Economic Studies of Moldova
Oleg STRATULAT*[2]*, PhD, Professor,
Academy of Economic Studies of Moldova

Actuality and purpose of work. Bitcoin is a currency that exists only virtually and has appeared due to the global financial crisis and development of technologiesof technologies. Cashless payments become more popular and in this context e-commerce has improved. There were Aanalized the ysis of bitcoin perspectives in the banking system, by emphasizing analyzing the strengths and weaknesses of this currency and the point of view of investors, central banks and commercial banks. The methods used. The methodological approaches used bymentioned in special literature were used. The results of the work. Analysis can be used to improve electronic commerce and cashless payments in Moldova, where cash is still very widely used.

Key words. *Bitcoin, cryptocurrency, blockchain, transactions, bank, investor.*

Actualitatea și scopul lucrării. Bitcoinul este o monedă care există doar în mediul electronic și a apărut în urma crizei financiare globale și datorită dezvoltării tehnologiilor informaționale. Plățile fără numerar devin tot mai populare, în acest context, evoluează comerțul electronic. Este studiată analiza perspectivelor utilizării bitcoinului în sistemul bancar, cercetate punctele forte și punctele slabe ale acestei monede, precum și opinia investitorilor, băncilor centrale și băncilor comerciale. Metode. Suportul metodologic este consituit din abordările folosite în literatura de specialitate. Rezultatele lucrării. Analiza poate fi aplicată în dezvoltarea comerțului electronic și a plăților fără numerar în Republica Moldova, unde numerarul este folosit pe larg.

Cuvinte-cheie. *Bitcoin, criptovalută, lanț în bloc, tranzacție, bancă, investitor.*

Актуальность и цель работы. Биткойн является валютой, которая существует только в электронном виде, которая появилась из-за мирового финансового кризиса и развития информационных технологий. Безналичные платежи становятся все более популярными и развивалась в этом контексте и электронная торговля. Анализ использования биткойн в банковской системе, анализируя сильные и слабые стороны этой валюты, а также точки зрения инвесторов, центральных банков и коммерческих банков. Используемые методы. Методологические подходы, которые используются в специализированной литературе. Результаты работы. Анализ может быть использован в целях развитии электронной торговли и безналичных платежей в Молдове, где наличные средства по-прежнему очень широко используются.

Ключевые слова. *Биткойн, криптовалюта, цепочка блоков, транзакция, банк, инвестор.*

JEL Classification: G24; E5; L81; O30.

Introduction. The modern technologies have changed the world of money and the essence of currency. Moreover, it has generated a new form of currency – cryptocurrency. Among these, the most highlitedhighlighted is the bitcoin.

The bitcoin phenomenon. Bitcoin is a virtual currency – cryptocurrency, invented by Satoshi Nakamoto in 2008. It seems that the disappointments regarding flat currencies – dollar, euro and others have reached a critical point. The evolution of this currency is amazing. At the beginning of 2015 there were over 14 million Bitcoin in circulation (Figure 1).

---

[1] © Mircea PLOTEANU, ploteanumircea@yahoo.com
[2] © Oleg STRATULAT, ostratulat@yahoo.com

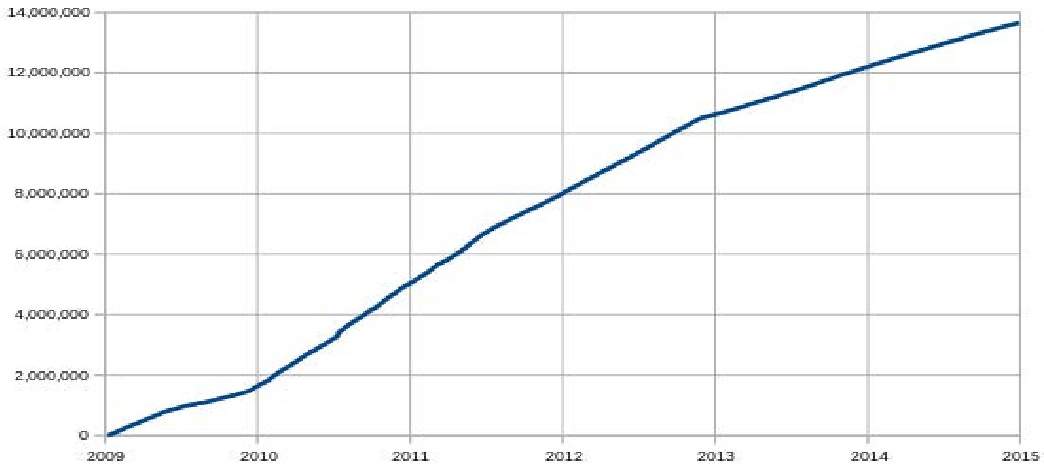


Fig. 1. Amount of bitcoins in circulation
Source: https://en.wikipedia.org/wiki/Bitcoin#/media/File:Total-bitcoins.svg [1].

From 2009, Bitcoin had a stable evolution until 2011, but from 2011 the exchange rate against the US dollar increased from $ 0.30 for a bitcoin (BTC), to about $ 17. In early 2011, a number of issues of entities that conduct transactions in dollars led to rapidly falling prices at $ 5 / BTC. 2011 and 2012 were periods of consolidation, and the exchange rate increased to 14 $/BTC.

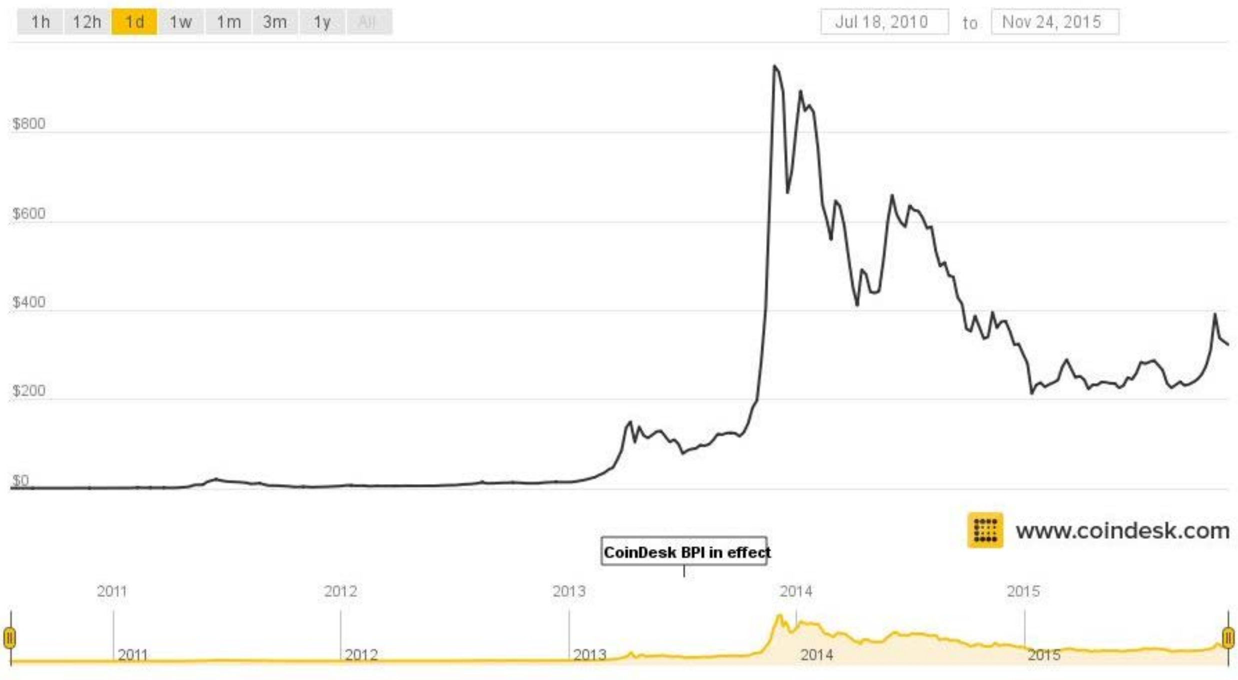


Fig. 2. The evolution of exchange rate, BTC/$ [2]
Source: http://www.coindesk.com/price/.

In 2013, the price of Bitcoin has exploded from 14 $/BTC in January to over $ 1000 in November - December 2013. An important role in this growing had the crisis in Cyprus (after blocking of the accounts in several banks). If 2013 was dominated by small bitcoin network "players", after involving of companies and investors the use of bitcoin has raised. The exploding rise of the exchange rate against the dollar has attracted the attention of authorities in many countries and bitcoin is not recognized as legal payment instrument. The exchange rate has declined steadily and was ranging several months between 550 to 650 $/BTC.

The whole structure is based on the ideas of bitcoin that Nakamoto defined as a chain of digital signatures, it is possible to consider the coin as a token digitally signed by the owner that desires to

transfer the currency. So each user transfer the coin to other subject in the network digitally signing a hash of the previous transaction and the public key of the next owner, the signature is then added to the end of the token.

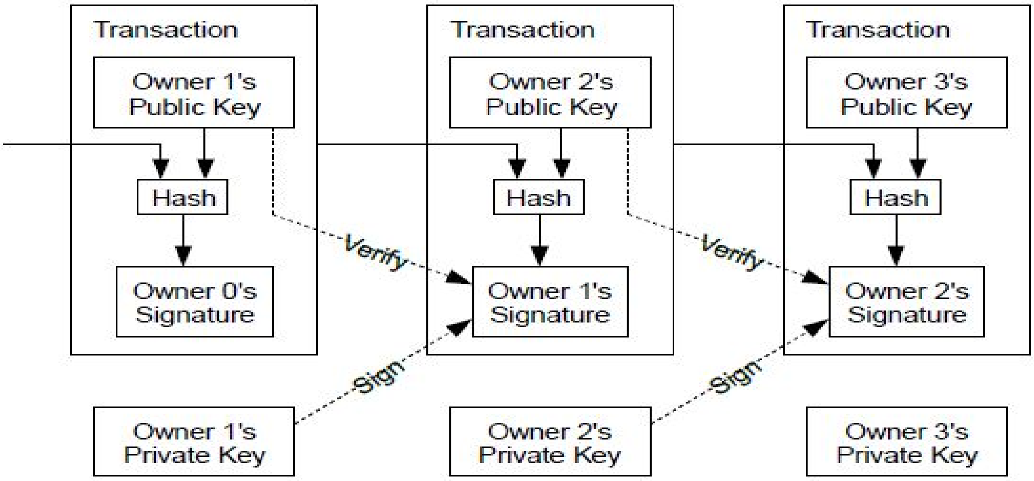


Fig. 3. The scheme of a bitcoin transaction

Source: http://www.4flush.com/bitcoin [3].

Only beneficiary could verify the previous transaction using its private key because the coin has been signed using its public key and this permit it to verify the chain of ownership. The described process has solved the problem of authentication of the payment, but we are not able to avoid the duplication of the transaction, in practice the circuit must avoid that the same coin could be used in multiple transactions.

The model is assured with the task of verifying that each coin is spent only once, this central authority is named “mint”. After each transaction the mint acquires the coin used to issue a new coin, in this way only the coins distributed directly from the mint are valid and only for them there is the assurance that have not already been spent.

Each new transaction is spread to all nodes of the network that collect the information related to the operation into a block. After verifying the time validity of the data the node spreads the block to other elements in the network.

The bitcoin software links to the network and generates the private and public keys necessary to take part to the process. The security of the model consists in the impossibility to exploit user’s private key from its public key, making impossible to impersonate the user. The keys could be moved from a PC to another because are stored in a file resident on the user’s PC.

Each transaction is characterized by beneficiary’s public key, owner private key and of course the amount of bitcoins that have to be transferred.

When a user A transfers the money to another user B prepares an information block which has the public key of B (the address) and the amount of coins to be transferred, by signing with the A private key. The information is then spread in the network and the nodes validate the signatures and the amount of numbers implicated before accepting it. When a node verifies the correctness of the transaction, it sends the details to the network to permit to other entities to verify them to permit to specific machines to add the transaction to a public record of transactions, and these machines are known as “*miners*”. The security level of the model is high, and makes impossible the creation of false transactions, each user can use only the bitcoins he has.

A transaction declares to the network that the holder of a number of bitcoins has accepted the transfer of some of bitcoins to another holder. The new owner can now spend these bitcoins by making another transaction that authorizes transfer to another owner, and so on, in a chain of ownership. Each transaction contains one or more “inputs”, which are debits against a bitcoin account. On the other side of the transaction, there are one or more “outputs”, which are credits added to a bitcoin account. The debits and credits do not necessarily add up to the same quantity.

The inflation program is initially planned for bitcoin and is known to all holders of bitcoin. Thus, inflation cannot be manipulated in order to affect the central spreading of value from ordinary users.

Bitcoin customer nodes transmit transaction, and the system is sending it in the network. Doubtful transactions are rejected by honest nodes. Transactions are free, but a fee could be paid to other nodes to facilitate transaction processing.

The risks of bitcoin use. Use of the bitcoin by banks is also questionable at the moment. But along the way, banks could use this money, such as Goldman Sachs and Standard Chartered, who published their recent reports that could use this money in the future. J. Panachyata, employee of BNP Paribas, says that use of Bitcoin will contribute to the development of global trade, in an article posted on his blog. Also Societe Generale is showing interest in bitcoin – the bank seeks an IT cryptocurrency specialist. Meanwhile, Swiss bank UBS has announced it will open a laboratory that will handle blockchain technology. US bank Goldman Sachs published a report in 2014 on virtual currencies, where is underlined the importance of cryptocurrencies. Spanish bank Santander says that thanks to blockchain technology, the costs could be reduced by 15-20 billion euro annually by 2022. A. Patwardhan from the bank Standard Chartered said that bitcoin will never become an alternative to fiat currencies [4]. Thus, we see that most commercial banks have an optimistic attitude towards this currency, while other analyzes market trends. But the central banks have taken a much tougher position against bitcoin, arguing that the use of cryptocurrencies implies shocking risks. With all its phenomenology, the use of bitcoin implies shocking risks. "Virtual currencies such as bitcoin, include potential risks to the financial system. Virtual currency is not a national currency and any currency and a payment acceptance is not binding legally. However, the virtual currency is not a form of electronic money within the meaning of Law no. 127/2011 regarding the activity of issuing electronic money", citing a National Bank of Romania release [5].

"The central bank shows that using virtual currency schemes as an alternative payment is potentially risky to the financial system because of lack regulation and supervision, money laundering, terrorism financing, price volatility and lack of adequate security", citing data from a report recently issued by the European Central Bank [6]. Unlike national currencies issued by central banks, bitcoin is generated by a complex chain of interactions between huge networks of computers worldwide. The coin has been criticized for its anonymous character and absence of regulation, there is concern about the possible use of it for financing terrorist activities or organized crime. Chair of FED, Janet Yellen, said the institution she leads cannot control a virtual currency [7], while countries like Russia and China have strongly restricted the use of bitcoin [8]. And some skeptical investors such as Warren Buffett, who said that in next 50 years the assets will have a higher value than paper money or bitcoin [9]. Famous economist Nouriel Roubini said that "Bitcoin is not a currency. It is a Ponzi scheme and a good conductor for criminal or illegal activities" [10]. Other investors such as Richard Brenson supports the idea of cryptocurrencies, believes in their future and in their potential [11]. If we are analyzing the topic from the security point of view, the issue is very huge. According to a study by Kapersky Lab [12], bitcoins can be stolen by wallet scammers and bitcoin softwares are attacked by malicious viruses.

Conclusions. Virtual currency schemes, such as bitcoin, are not full forms of money as usually defined in literature. Anyway, these schemes may replace banknotes, scriptural money and e-money in some situations. For the tasks of central banks, the materialization of these risks depends on the amount issued for the respective schemes, their bond to the real economy, including through regulated institutions implied with cryptocurrencies schemes, their traded volume and on user acceptance. Participation in such schemes exposes users not only to key payment system-like risks but also to other risks coming from the characteristics of cryptocurrencies. In particular, users are exposed to exchange rate risk related to high volatility, to counterparty risk related to the anonymity of the beneficiary and to investment fraud risk related to the absence of transparency. So there are both general and specific ways in which users could lose their whole virtual money. Some aspects of these risks are peculiar to the cryptocurrency concept and the risks mostly remain unmitigated by legislation, regulation or supervision.

The reactions from governments to the phenomenon are different, partly depending on the part of the world these originate from and on the type of authority. Responses differ from warnings about risks, statements and clarifications on the legal status, licensing and supervision of cryptocurrency-related activities, or the interdiction of those.

To conclude, we can say that the future of bitcoin is uncertain because it exists only in virtual environment and has a decentralized character. Commercial banks see a perspective in bitcoin, but do not rush to accept the payment instrument and analyze trends. But central banks have taken a tough stance against bitcoin, because the currency has a decentralized character and risks, such as money laundering, terrorist financing and anonymity.

REFERENCES

1. Bitcoin [accesat 02 septembrie 2015]. Disponibil: https://en.wikipedia.org/wiki/Bitcoin#/media/File:Total-bitcoins.svg
2. Bitcoin Price Index Chart [accesat 02 septembrie 2015]. Disponibil: http://www.coindesk.com/price/
3. GILL, T.J. Bitcoins. The Future of Currency*?* [accesat 02 septembrie 2015]. Disponibil: http://www.4flush.com/bitcoin
4. PEREZ, Yessi Bello. 8 Banking Giants Embracing Bitcoin and Blockchain Tech, 27 july 2015. [accesat 02 septembrie 2015]. Disponibil: http://www.coindesk.com/8-banking-giants-bitcoin-blockchain/
5. BANCA NAŢIONALĂ A ROMÂNIEI. Comunicat referitor la schemele de monedă virtuală, 11 martie 2015 [accesat 02 septembrie 2015]. Disponibil: http://www.bnr.ro/page.aspx?prid=10016
6. EUROPEAN CENTRAL BANK. Virtual currency schemes – a further analysis. Frankfurt am Main, Germany, 2015. 37 p. ISBN 978-92-899-1560-1 [accesat 02 septembrie 2015]. Disponibil: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
7. YELLEN, Janet. Federal Reserve has no authority to regulate Bitcoin, 27 february 2014 [accesat 8 septembrie 2015]. Disponibil: http://www.theguardian.com/business/2014/feb/27/janet-yellen-federal-reserve-no-authority-regulate-bitcoin
8. SMART, Evander. Top 10 Countries in Which Bitcoin is banned, 27 may 2015 [accesat 02 septembrie 2015]. Disponibil: https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/
9. БАФФЕТТ, Уоррен. Активы лучше денег в следующие 50 лет. 2014, 3 martie 2014 [accesat 02 septembrie 2015]. Disponibil: http://www.vestifinance.ru/articles/40146
10. ROUBINI, Nouriel. Bitcoin Is a ‘Ponzi Game’, 10 mars 2014 [accesat 02 septembrie 2015]. Disponibil: http://blogs.wsj.com/moneybeat/2014/03/10/nouriel-roubini-bitcoin-is-a-ponzi-game/
11. BRANSON, Richard. How digital currency could transform the world, 13 november 2014 [accesat 03 septembrie 2015]. Disponibil: http://www.virgin.com/richard-branson/how-digital-currency-could-transform-the-world
12. BĂDĂRĂU, Elena. Securitatea naţională şi diminuarea riscurilor ciberameninţărilor = National security and reducing of cyber-attack risks. In: Economie şi Sociologie = Economy and Sociology. 2014, no. 4, pp. 85-103. [accesat 03 septembrie 2015]. Disponibil: http://ince.md/ro/complexul-editorial/publicacii-periodice/reviste-tiinifice/economie-si-sociologie/

Recommended for publication: 14.09.2015

BEYOND BITCOIN: ISSUES IN REGULATING BLOCKCHAIN TRANSACTIONS

TREVOR I. KIVIAT†

ABSTRACT

The buzz surrounding Bitcoin has reached a fever pitch. Yet in academic legal discussions, disproportionate emphasis is placed on bitcoins (that is, virtual currency), and little mention is made of blockchain technology—the true innovation behind the Bitcoin protocol. Simply, blockchain technology solves an elusive networking problem by enabling "trustless" transactions: value exchanges over computer networks that can be verified, monitored, and enforced without central institutions (for example, banks). This has broad implications for how we transact over electronic networks.

This Note integrates current research from leading computer scientists and cryptographers to elevate the legal community's understanding of blockchain technology and, ultimately, to inform policymakers and practitioners as they consider different regulatory schemes. An examination of the economic properties of a blockchain-based currency suggests the technology's true value lies in its potential to facilitate more efficient digital-asset transfers. For example, applications of special interest to the legal community include more efficient document and authorship verification, title transfers, and contract enforcement. Though a regulatory patchwork around virtual currencies has begun to form, its careful analysis reveals much uncertainty with respect to these alternative applications.

---

† Duke University School of Law, J.D. / LL.M. expected 2016; Syracuse University, B.S. 2011. I have no financial interest in bitcoin. My thanks in completing this Note are many: to Sheldon Thomas, for introducing me to bitcoin and for many lively conversations on this topic; to Professor Campbell R. Harvey, for inviting me to workshop early versions of this Note in his Cryptoventures course; to Reuben Grinberg and John Weinstein, for insightful comments and mentorship; to the Bluebook ninjas of the *Duke Law Journal*, for their outstanding contributions; and to my family, for their endless love, patience, and support.

The circulation of confidence is better than the circulation of money.

– James Madison[1]

INTRODUCTION

On December 26, 2014, three million homes nationwide tuned in to watch the North Carolina State Wolfpack take on the University of Central Florida Knights in the Bitcoin St. Petersburg Bowl—the first of several bitcoin-branded, postseason college bowl games.[2] ESPN's online presale, held open to sports fans across the nation, involved one catch: prospective attendees could only purchase the tickets with bitcoin.[3] This episode was the first of many that collectively exemplify the mainstreaming of virtual currencies—an atmosphere most recently dominated by the acts of financial players,[4] such as the New

1. Statement of James Madison at the Virginia Convention (June 20, 1788), *in* 4 THE DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 538 (Jonathan Elliot ed., 2d ed. 1836). As this Note illustrates, Bitcoin's core innovation is not the controversial "virtual currency"; rather, it is the facilitation of "trustless" electronic transactions. In other words, blockchain transactions allow each party to independently verify that it is not being defrauded, without the involvement of a trusted intermediary, such as a bank or other financial institution. This is the circulation of confidence.

2. Tony Gallippi, *ESPN and BitPay Enter 3-Year Deal To Produce NCAA Bowl Game*, BITPAY BLOG (June 18, 2014), http://blog.bitpay.com/2014/06/18/espn-and-bitpay-enter-3-year-deal-to-produce-ncaa-bowl-game.html [http://perma.cc/9RAT-WMDS].

3. Tony Gallippi, *Get Ready for the Bitcoin Bowl*, BITPAY BLOG (Oct. 15, 2014), https://blog.bitpay.com/get-ready-for-the-bitcoin-bowl [http://perma.cc/H6QF-GQLB].

4. *See, e.g.*, Clint Boulton, *BNY Mellon Explores Bitcoin's Potential*, WALL ST. J. (Apr. 5, 2015, 6:19 PM), http://blogs.wsj.com/cio/2015/04/05/bny-mellon-explores-bitcoins-potential [http://perma.cc/9NQL-N9FV] (describing how Bank of New York Mellon is experimenting with blockchain technology); Grace Caffyn, *Barclays Trials Bitcoin Tech With Pilot Program*, COINDESK (June 22, 2015, 3:32 PM), http://www.coindesk.com/barclays-trials-bitcoin-tech-with-pilot-program [http://perma.cc/DDH2-J5ZU] (detailing Barclay's signing off on a proof-of-concept to trial blockchain technology); Grace Caffyn, *RBS Trials Ripple as Part of £3.5 Billion Tech Revamp*, COINDESK (June 26, 2015, 2:03 PM), http://www.coindesk.com/rbs-trials-ripple-part-3-5-billion-tech-revamp [http://perma.cc/PZS8-5NK8] (describing Royal Bank of Scotland's efforts to integrate blockchain-based technology as part of a technological revamp); *Nasdaq Launches Enterprise-Wide Blockchain Technology Initiative*, NASDAQ (May 11, 2015), http://ir.nasdaq.com/releasedetail.cfm?releaseid=912196 [http://perma.cc/GH2Z-KQGZ] (detailing Nasdaq's blockchain technology initiative); Nathanial Popper, *When Goldman Sachs Began Flirting with Bitcoin*, AM. BANKER (May 21, 2015), http://www.americanbanker.com/bankthink/when-goldman-sachs-began-flirting-with-bitcoin-1074472-1.html [http://perma.cc/3CBJ-7AUY] (profiling Goldman Sachs's interest in blockchain technology).

York Stock Exchange (NYSE), and state regulators,[5] such as New York's Department of Financial Services (NYDFS).

Bitcoin discussions largely focus on the technology's well-publicized growing pains: wild price volatility;[6] fraudulent investment schemes;[7] multimillion dollar hacks;[8] and the infamous Silk Road case[9]—an episode that resulted in a life sentence for Ross Ulbricht,[10] drug kingpin of the deep web,[11] and the indictment of two federal agents.[12] Accordingly, some intelligent and well-respected detractors

5. New York was first. The list now includes California and North Carolina. Additionally, legislators in Connecticut, New Hampshire, New Jersey, and Pennsylvania are considering various proposals. Peter Van Valkenburgh, *Tracking Bitcoin Regulation State by State*, COIN CENTER (June 2, 2015), https://coincenter.org/2015/06/tracking-bitcoin-regulation-state-by-state [https://perma.cc/U646-8K59].

6. *See Market Price (USD)*, BLOCKCHAIN.INFO, https://blockchain.info/charts/market-price [http://perma.cc/JPQ9-AZNR] (providing historical and real-time price data).

7. *See, e.g.*, SEC v. Shavers, No. 4:13-CV-416, 2014 WL 4652121, at *14, *21–25 (E.D. Tex. Sept. 18, 2014) (finding an interest in a bitcoin-based Ponzi scheme to be an "investment contract" for purposes of U.S. securities laws and imposing civil monetary penalties under the Securities Act); Press Release, U.S. Dep't of Justice, Manhattan U.S. Attorney Announces Charges Against Two Florida Men For Operating An Underground Bitcoin Exchange (July 21, 2015), http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-two-florida-men-operating-underground [https://perma.cc/T3QF-D97T] (describing charges brought against defendants who operated a federal credit union as a captive bank for their illegal business).

8. *See, e.g.*, Robert McMillan, *$1.2m Hack Shows Why You Should Never Store Bitcoins on the Internet*, WIRED (Nov. 7, 2013, 3:49 PM), http://www.wired.com/2013/11/inputs [http://perma.cc/FD5L-2ZCU] (reporting on a hack suffered by inputs.io, a wallet software provider); Amir Mizroch, *Large Bitcoin Exchange Halts Trading After Hack*, WALL ST. J.: DIGITS BLOG (Jan. 6, 2015, 4:13 AM), http://blogs.wsj.com/digits/2015/01/06/large-bitcoin-exchange-halts-trading-after-hack [http://perma.cc/5L8K-LZZX] (reporting on a hack on "[o]ne of the largest bitcoin exchanges").

9. *See generally* Joshuah Bearman, *The Rise and Fall of Silk Road: Part I*, WIRED (Apr. 2015), http://www.wired.com/2015/04/silk-road-1 [http://perma.cc/LE7G-HM6T] (detailing the Silk Road case); Joshuah Bearman, *The Rise and Fall of Silk Road: Part II*, WIRED (May 2015), http://www.wired.com/2015/05/silk-road-2 [https://perma.cc/9XH5-XFLK] (same).

10. Press Release, Dep't of Justice, Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced in Manhattan Federal Court to Life in Prison (May 29, 2015), http://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison [http://perma.cc/9LBY-X8XF].

11. The deep web is a "portion of the Internet that is hidden from conventional search engines, as by encryption," such as the Tor network, often used for illegal or criminal activity. *See Deep Web*, DICTIONARY.COM, http://www.dictionary.reference.com/browse/deep-web?s=t [http://perma.cc/2KMN-B42K]. For an interactive, nautical-themed representation of this concept, see *What Is the Deep Web?*, CNN MONEY (Mar. 10, 2014, 9:18 AM), http://money.cnn.com/infographic/technology/what-is-the-deep-web [http://perma.cc/8R3B-4ECT].

12. Press Release, Dep't of Justice, Former Federal Agents Charged with Bitcoin Money Laundering & Wire Fraud (Mar. 30, 2015), https://www.fbi.gov/sanfrancisco/press-releases/2015/former-federal-agents-charged-with-bitcoin-money-laundering-and-wire-fraud [https://perma.cc/

have called it a "bubble,"[13] and others have gone so far as to call it "evil."[14] Nevertheless, technologists and business leaders have declared it "better than currency,"[15] citing its promise to lower transaction costs,[16] transform developing economies,[17] and generally "reshape [the financial] system."[18] Simply put, sensationalism in this area is high.[19] Perhaps this is encouraged by the facts, which read like a science fiction novel, blurring the physical and digital worlds:[20] A pseudonymous inventor[21] releases a cryptographic[22] technology that

---

4J3P-V248].

13. Robert J. Shiller, *In Search of a Stable Electronic Currency*, N.Y. TIMES, Mar. 1, 2014, at BU4. Professor Shiller was awarded the 2013 Nobel Prize in Economic Sciences along with Professors Eugene Fama and Lars Peter Hansen for their research into market prices and asset bubbles. *The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2013*, NOBELPRIZE.ORG (Oct. 28, 2015), http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2013 [http://perma.cc/6XEW-GUG6].

14. Paul Krugman, *Bitcoin is Evil*, N.Y. TIMES: CONSCIENCE OF A LIBERAL (Dec. 28, 2013, 2:35 PM), http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil [http://perma.cc/8K5G-W62Y].

15. Kim Lachance Shandrow, *Bill Gates: Bitcoin is 'Better than Currency'*, ENTREPRENEUR (Oct. 3, 2014), http://www.entrepreneur.com/article/238103 [http://perma.cc/LTM4-UUJJ].

16. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-496, VIRTUAL CURRENCIES: EMERGING REGULATORY, LAW ENFORCEMENT, AND CONSUMER PROTECTION CHALLENGES 23 (2014).

17. *See* JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 14–15 (2013) (describing bitcoin's potential to improve the lives of the world's most impoverished individuals); Kyle Torpey, *Five Economies that Could Actually Use Bitcoin*, VICE: MOTHERBOARD (Apr. 30, 2014, 1:30 PM), http://motherboard.vice.com/blog/five-economies-that-could-actually-use-bitcoin [http://perma.cc/G34G-QCV9] (profiling prospects for bitcoin to support financial modernization in developing countries).

18. Marc Andreesen, *Why Bitcoin Matters*, N.Y. TIMES: DEALBOOK (Jan. 21, 2014, 11:54 AM), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters [http://perma.cc/HW64-TH PB].

19. Here is a sampling of the "greatest hits" of sensationalist headlines: John Mauldin, *Is Bitcoin the Future?*, FORBES (Dec. 1, 2014, 11:29 AM), http://www.forbes.com/sites/johnmauldin/2014/12/01/is-bitcoin-the-future/ [https://perma.cc/LJ97-FZEJ]; Jose Pagliery, *Ron Paul: Bitcoin Could 'Destroy the Dollar'*, CNN MONEY (Dec. 4, 2013, 12:01 PM), http://money.cnn.com/2013/12/04/technology/bitcoin-libertarian [http://perma.cc/4D2X-V6MW]; Jonathan M. Trugman, *Welcome to 21st-Century Ponzi Scheme: Bitcoin*, N.Y. POST (Feb. 15, 2014, 5:08 PM), http://nypost.com/2014/02/15/welcome-to-21st-century-ponzi-scheme-bitcoin [http://perma.cc/R8FP-9ZRH]; Tim Worstall, *So, That's the End of Bitcoin Then*, FORBES (June 20, 2011, 4:42 AM), http://www.forbes.com/sites/timworstall/2011/06/20/so-thats-the-end-of-bitcoin-then [http://perma.cc/3AE4-9L4L].

20. For a particularly entertaining work blending the real and synthetic, see PHILIP K. DICK, DO ANDROIDS DREAM OF ELECTRIC SHEEP? (1968).

21. *See* Hiroko Tabuchi, *Will the Real Satoshi Nakamoto Please Stand Up?*, N.Y. TIMES: DEALBOOK (Mar. 11, 2014, 3:57 PM), http://dealbook.nytimes.com/2014/03/11/will-the-real-satoshi-nakamoto-please-stand-up [https://perma.cc/5739-DSVB] (exploring the intrigue regarding the true identity of the Bitcoin architect).

incentivizes armies of supercomputers[23] to mine digital assets[24] that can be traded for real-world goods and services.[25]

Further, authors almost exclusively focus on bitcoin as a currency system. For example, authors have weighed the costs and benefits of transacting with virtual currencies,[26] considered the sustainability of virtual currencies,[27] and contemplated the application of existing regulatory schemes to virtual currency.[28] Missing from the dialogue is a deeper perspective on the technology.

This Note offers that perspective. Primarily, it expands on contemporary academic literature by highlighting the conceptual distinction between bitcoins (that is, virtual currency) and the "blockchain,"[29] the Bitcoin platform's key technological innovation. It

---

22. Cryptography is "the scientific study of techniques for securing digital information, transactions, and distributed computations." JONATHAN KATZ & YEHUDA LINDELL, INTRODUCTION TO MODERN CRYPTOGRAPHY: PRINCIPLES AND PROTOCOLS 3 (2007).

23. *Bitcoin: The Magic of Mining*, THE ECONOMIST, Jan. 10, 2015, at 58, http://www.economist.com/node/21638124 [http://perma.cc/UB2F-2EL7]; Ashlee Vance & Brad Stone, *The Bitcoin-Mining Arms Race Heats Up*, BLOOMBERG BUSINESSWEEK (Jan. 9, 2014), http://www.businessweek.com/articles/2014-01-09/bitcoin-mining-chips-gear-computing-groups-competition-heats-up [http://perma.cc/6XK3-KVYJ].

24. A digital asset is essentially any digital file with economic properties that generate value, such as consumption or transfer rights. TOBIAS BLANKE, DIGITAL ASSET ECOSYSTEMS: RETHINKING CROWDS AND CLOUDS 8 (2014).

25. Over 100,000 merchants accept payments in bitcoin as of the publication of this Note. Anthony Cuthbertson, *Bitcoin Now Accepted by 100,000 Merchants Worldwide*, INT'L BUS. TIMES (Feb. 4, 2015, 3:34 PM), http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613 [http://perma.cc/Y26K-FMCB].

26. *See, e.g.*, Joshua J. Doguet, Comment, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119, 1130 (2013) (arguing that bitcoin benefits users by cutting out financial intermediaries—that is, lowers transaction costs—which makes possible even smaller transactions).

27. *See* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 174–81 (2012) (considering the sustainability of bitcoin and concluding that bitcoin is not doomed).

28. *See, e.g.*, Ruoke Yang, *When is Bitcoin a Security Under U.S. Securities Law?*, 18 J. TECH. L. & POL'Y 99, 99 (2014) (federal securities regulation); Kelsey L. Penrose, Note, *Banking On Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 N.C. BANKING INST. J. 529, 529 (2014) (anti-money-laundering schemes); *see also* Paul H. Farmer, Jr., Comment, *Speculative Tech: The Bitcoin Legal Quagmire & The Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85, 86 (2014) (exploring the appropriate legal definition for "bitcoins," based upon their intended and actual use); Matthew Kien-Meng Ly, Note, *Coining Bitcoin's "Legal-Bits": Examining The Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J.L. & TECH. 587, 596 (2014) (contemplating whether and which existing legal frameworks may be used to regulate bitcoin).

29. The blockchain is also referred to as the "Bitcoin protocol." *Drawing Distinction Between the Uppercase "B" and Lowercase "b" in Bitcoin*, BLOCKCHAIN (Dec. 29, 2014), http://blog.blockchain.com/2014/12/29/drawing-the-distinction-between-the-uppercase-b-and-

does this by integrating current research from leading computer scientists and cryptographers.[30] And its ultimate aim is to elevate the legal community's understanding of blockchain technology and, ultimately, to inform policymakers and practitioners as they consider different regulatory regimes.

In short, the blockchain is a "trustless" technology.[31] "Trustless" means—for the first time in history—exchanges for value over a computer network can be verified, monitored, and enforced without the presence of a trusted third party or central institution.[32] Because the blockchain is an authentication and verification technology,[33] it can enable more efficient title transfers and ownership verification.[34] Because it is programmable, it can enable conditional "smart" contracts.[35] Because it is decentralized, it can perform these functions with minimal trust without using centralized institutions.[36] Because it is borderless and frictionless, it can provide a cheaper, faster infrastructure for exchanging units of value.[37]

Simply, blockchain technology has broad implications for how we transact, and the potential for innovation is hard to overstate.[38] Regardless of one's opinion on the merits of virtual currencies, financial regulators must develop a better understanding of blockchain technology's impact potential as they continue to engage in its pragmatic regulation.

---

lowercase-b-in-bitcoin [http://perma.cc/6TGY-9P6W]. A capital "B" is associated with the protocol and the community; for example, "The Bitcoin ecosystem consists of a wide swath of activities, businesses, and services." A lowercase "b" is associated specifically with the virtual currency; for example, "My favorite local coffee shop now accepts payments in bitcoin."

30. *See supra* note 22 (defining cryptography).

31. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 8 (2009), https://bitcoin.org/bitcoin.pdf [https://perma.cc/MW6Y-WSCR].

32. *Id*.

33. ADAM BACK ET AL., ENABLING BLOCKCHAIN INNOVATIONS THROUGH PEGGED SIDECHAINS 7 (2014), http://www.blockstream.com/sidechains.pdf [http://perma.cc/995Y-ALF8].

34. *Id*. at 4, 15–16.

35. *Id*. at 4.

36. NAKAMOTO, *supra* note 31, at 1.

37. *See* TIM SWANSON, GREAT CHAIN OF NUMBERS: A GUIDE TO SMART CONTRACTS, SMART PROPERTY AND TRUSTLESS ASSET MANAGEMENT 67 (2014) (describing math-based "cryptocurrencies" such as bitcoin as an alternative to the often slow and expensive money transfers).

38. One might use venture capital investment data as a rough proxy for perceived innovation opportunities in this area. Total investments in the technology—both venture capital and strategic—are estimated to be over $1 billion. Jose Pagliery, *Record $1 Billion Invested in Bitcoin Firms So Far*, CNN MONEY (Nov. 3, 2015, 12:56 PM), http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested [http://perma.cc/88HT-GGKB].

This Note proceeds in three Parts. Part I introduces blockchain technology and its most widely understood application: money transfers and payments with bitcoin. First, it explains how blockchain transactions occur and why this technology is highly innovative. Second, it explores bitcoin's economic properties and situates the currency within the long evolution of monetary technology. Drawing on economic perspectives, it highlights the benefits and drawbacks of a blockchain-based currency like bitcoin. Part I concludes that the technology's most valuable utility lies beyond bitcoin—in other words, not as a currency but as an exchange medium for digital-asset transfers.

Part II surveys the emerging regulatory landscape, which is heavily premised on the technology's singular application as a virtual currency. First, it explains the current federal scheme—a patchwork of bitcoin-specific guidance and rulings from the Financial Crimes Enforcement Network (FinCEN), paired with the Commodity Futures Trading Commission's (CFTC) oversight authority and the Securities and Exchange Commission's (SEC) enforcement capabilities, which both apply in highly limited circumstances. Next, it explores recent state action—namely, New York's BitLicense, with special attention to its key provisions and ambiguities.[39] At each layer of regulation, it examines open issues that present uncertainty and opportunity for further clarification.

Part III raises issues presented by blockchain technology beyond virtual currency—beyond bitcoin. It covers applications of special interest to the legal community including more efficient contracts, document and authorship verification, and title transfers. It also explores more advanced aspects of the technology, an understanding of which is essential for sensible policy making in this area. After exploring the vistas beyond bitcoin, this Note concludes by offering thoughts on how caution and restraint might be exercised in the law to facilitate technological and economic growth.

---

39. As this Note goes to press, other states are taking significant steps—most notably, California and North Carolina. Valkenburgh, *supra* note 5. For timely updates relating to regulation of bitcoin and other virtual currencies, see *Virtual Currency Regulation Resources*, DAVIS POLK & WARDWELL LLP, http://bitcoin-reg.com [http://perma.cc/RAY6-4QGJ].

I. THE BLOCKCHAIN, PART 1: BITCOIN, A BLOCKCHAIN-BASED CURRENCY

Experiments in currency are as old as commerce and civilization itself.[40] Today, most currencies—the U.S. dollar included—are fiat currencies.[41] Fiat currencies are not backed by physical assets;[42] rather, they are backed by the promise of their issuing government.[43] Commodity monies, by contrast, are backed by a tradable, naturally scarce resource with value beyond its use in trade.[44] Gold or silver, for example, backed the U.S. dollar for much of our nation's history.[45] This Section explains why bitcoin, the blockchain-based "virtual currency," does not fit comfortably into either of these traditional categories.

First, this Section answers the fundamental question, "What is bitcoin?" by explaining the lifecycle of a blockchain transaction. Second, it examines the economic properties of an artificial commodity like bitcoin as compared to well-known and widely traded physical commodities and traditional fiat currencies. Finally, it highlights the special properties of this technology—core features that not only enable blockchain-based currencies but also hold vast potential for applications beyond bitcoin.

40. *See generally* GLYN DAVIES, A HISTORY OF MONEY: FROM ANCIENT TIMES TO MODERN DAY (3d ed. 2002) (documenting the history of currency).

41. *Id*. at 355.

42. In other words, the holder of a paper Federal Reserve Note does not have the right to any amount of an asset—for example, gold or silver, from the government. *Id*. at 642.

43. *See* 31 U.S.C. § 5103 (2012) ("United States coins and currency . . . are legal tender for all debts, public charges, taxes, and dues.").

44. 1 JOHN MAYNARD KEYNES, A TREATISE ON MONEY: THE PURE THEORY OF MONEY 14 (1930). Monetary economists sometimes refer to this as "intrinsic value"—think gold, silver, tobacco, and cocoa beans. ARTHUR O'SULLIVAN & STEVEN M. SHEFFRIN, ECONOMICS: PRINCIPLES IN ACTION 246 (2003).

45. *See generally* George Selgin, *The Rise and Fall of the Gold Standard in the United States*, CATO INST. POL'Y ANALYSIS (June 20, 2013), http://www.cato.org/sites/cato.org/files/pubs/pdf/pa729_web.pdf [http://perma.cc/C3YT-WT4Y] (reviewing the history of the gold standard in the United States).

A. The Blockchain: "Triple-Entry Accounting"[46] on a Transparent, Public Ledger

In the physical world, security requires locks, vaults, and signatures; in the digital world, it requires cryptography, or techniques for securing digital information and transactions.[47] The blockchain is a cryptographic technology.[48] It is the core innovation driving the bitcoin currency system, and it solves an important technological problem. For the first time ever, secure electronic transfers of value can occur without the presence of a trusted third party.[49] By contrast, outside of the blockchain, electronic transfers of value require financial intermediaries—for example, commercial banks, brokerages, or PayPal—to establish trust and security in the transaction.[50] Such institutions establish trust and security by preserving a centralized ledger[51] to track account holders' balances and, ultimately, vouch for a transaction's authenticity.[52] Without intermediaries, electronic units of value—dollars, for instance—can be copied and spent twice, just as any digital document can be copied ad infinitum.[53] This "double spending problem"[54] has riddled programmers for decades.[55]

---

46. Modern financial accounting is a double-entry system—a system of recordkeeping that allows firms to maintain records of what the firm owns and owes and what the firm has earned and spent over any given period of time. Triple-entry accounting refers to the idea that transactions on the blockchain are essentially accounting entries that are cryptographically sealed, preventing tampering and enabling near-real-time auditing.

47. KATZ & LINDELL, *supra* note 22, at 3.

48. NAKAMOTO, *supra* note 31, at 1.

49. *Id*. at 8.

50. *See* ORG. FOR ECON. CO-OPERATION & DEV., THE ROLE OF INTERNET INTERMEDIARIES IN ADVANCING PUBLIC POLICY OBJECTIVES 173–83 (2011) (chronicling the development and growth of online payment intermediaries).

51. This used to be a physical ledger; now it is a centralized server network. *See* BRIJENDRA SINGH, NETWORK SECURITY AND MANAGEMENT 323 (3d ed. 2012) (describing how centralized server networks are utilized for Internet banking).

52. *Id*.

53. The recorded music industry is still recovering from the painful implications of this fact. *See* David Byrne, *David Byrne's Survival Strategies for Emerging Artists—and Megastars*, WIRED (Dec. 18, 2007), http://archive.wired.com/entertainment/music/magazine/16-01/ff_byrne?currentPage=all [http://perma.cc/7EPD-Q8L9] (explaining how peer-to-peer file sharing transformed the economic model of the recorded music industry).

54. The double-spending problem is also referred to as the "Two Generals' Problem," and is illustrated best through the following hypothetical: Imagine two generals, each preparing his troops to attack a common enemy. Each squadron is situated on separate hills, flanking the enemy. The generals can communicate only by courier. Each message sent carries a risk of interception by the enemy. While the two generals have agreed to attack, they have not agreed

Blockchain technology enables secure electronic transactions without a centralized ledger and without double spending.[56] Instead of a centralized ledger, it makes a collective accounting by distributing a shared (that is, decentralized) public ledger—a complete record of all past transactions on the network.[57] This ledger is the blockchain.[58] When two parties wish to engage in a transaction, they must broadcast it to the entire network,[59] effectively asking network participants to determine its authenticity.[60] The following example illustrates this process.

Party A begins by broadcasting a message to the network signaling the terms of the agreement.[61] For example, "I, Party A, am giving Party B one bitcoin." Next, Party B accepts the transaction by broadcasting its acceptance to the entire network[62] and asking network participants to determine the authenticity of the transaction.[63] The network automatically validates the transaction—or guards against the threat of double spending—through a "proof-of-work" validation system.[64] If the transaction is validated, the ledger is

---

upon a time. Assume that a successful attack requires both squadrons to attack the city simultaneously. The issue, then, is that the two generals must agree on an attack time, and each general must know that the other general knows they have agreed. This is difficult because acknowledgement of receipt can be lost as easily as the original message. Thus, a potentially infinite chain of messages is required to reach consensus. *See* Jim Gray, IBM RES. LABORATORY, *Notes on Data Base Operating Systems*, *in* LECTURE NOTES IN COMPUTER SCIENCE 394, 465 (G. Goos & J. Hartmanis eds., 1978), http://research.microsoft.com/en-us/um/people/gray/papers/DBOS.pdf [http://perma.cc/C5ZV-RZ7C] (coining the name "Two Generals' Problem"); *see also* E. A. Akkoyunlu, K. Ekanadham & R. V. Huber, *Some Constraints and Tradeoffs in the Design of Network Communications*, *in* PROCEEDINGS OF THE FIFTH ACM SYMPOSIUM ON OPERATING SYSTEMS PRINCIPLES 67, 73 (J.C. Browne & Juan Rodriguez-Rosell eds., 1975) (documenting the problem for the first time).

55. *See* Gray, *supra* note 54, at 466 (describing the problem as having no solution in 1978).

56. NAKAMOTO, *supra* note 31, at 8.

57. *Id*. at 3.

58. *See id*. (explaining that transactions are recorded in a series of blocks). Although the term "blockchain" was not used in Nakamoto's original paper, it has become synonymous with this technology because transaction data is encoded in blocks that, together, make a chain of all past transactions. BACK ET AL., *supra* note 33, at 3.

59. BACK ET AL., *supra* note 33, at 3–4.

60. *Id*.

61. *Id.*

62. NAKAMOTO, *supra* note 31, at 3. "Broadcasting," in telecommunication and information theory, refers to the method of transferring a message to all recipients or network participants simultaneously. ANDREW S. TANENBAUM & DAVID J. WETHERALL, COMPUTER NETWORKS 17 (5th ed. 2012). In this case, that message is, "I accept the transaction."

63. NAKAMOTO*, supra* note 31, at 4.

64. *Id*. at 3–4.

updated[65] and network users' blockchain records are collectively updated.[66] In other words, once a transaction has been recorded in this transparent public ledger, that transaction cannot be changed after the fact (unless it is matched with a second offsetting transaction).[67]

The proof-of-work validation system is essentially a competition among network participants to validate transactions.[68] Network users participate in this competition by exercising computational power.[69] Under this system, a user's ability to improperly influence validation—to double spend—is limited by the total proportional computation power he can harness.[70] Users are incentivized to bear the computational costs of validation because successful participants are rewarded with new bitcoin.[71] Accordingly, new bitcoins are said to have been "mined," with the "[computational] time and electricity that is expended" as "analogous to gold miners expending resources to add gold to circulation."[72] Eventually there will be nothing left to mine because the total outstanding supply is limited.[73] When that

65. Alternatively, a request for a dishonest transaction falls off the chain and therefore the transaction never occurs.

66. BACK, *supra* note 33, at 3–4. In this respect, the blockchain can be thought of as a historical record of all transactions that have occurred on the network.

67. *Id*. at 1. *But see Stop Saying Bitcoin Transactions Aren't Reversible*, ELI DOURADO (Dec. 4, 2013), https://elidourado.com/blog/bitcoin-arbitration [https://perma.cc/5XW3-YU5Y] (describing advanced features of blockchain technology that may essentially provide users with the ability to encode transactions to include arbitration and similar dispute-resolution services).

68. NAKAMOTO, *supra* note 31, at 3. The transactions are time-stamped to ensure validity. *Id.* at 2.

69. *Id*. at 2.

70. "Computation power" essentially refers to how fast a machine can perform an operation. *See generally* AKEO ADACHI, FOUNDATIONS OF COMPUTER THEORY (1990). The merits of this validation scheme are apparent when compared to a hypothetical alternative. Imagine a scheme in which validation is influenced by the number of network identities the user controls instead of his computational power. Although the marginal cost of acquiring more identities is nearly zero, the marginal cost of amassing greater computational power is quite significant. Accordingly, the scheme that properly deters participants from cheating, or double spending, is the one that raises the costs of cheating to a point of impracticability. *See* NAKAMOTO, *supra* note 31, at 4, 8 (asserting that the structure of Bitcoin makes cheating "computationally impractical").

71. NAKAMOTO, *supra* note 31, at 4. Similarly, users are disincentivized from double spending because the economic cost of doing so, as measured by the computation power required, outweighs the benefits that could be gained in a given transaction.

72. *Id.*

73. Grinberg, *supra* note 27, at 163 (explaining that the rate of bitcoins issued declines by half every four years and that the number of bitcoins approaches but never reaches the total supply of 21 million).

happens, the incentive to validate transactions will likely be transaction fees.[74] Importantly, this is an open-source protocol, meaning open innovation can occur around the technology's various parameters.[75]

In sum, the blockchain establishes trust between two parties to a transaction through both a decentralized public ledger and a cryptographic mechanism that ensures transactions cannot be changed after the fact.[76] One can easily see why the creator of this technology called it "purely peer-to-peer . . . electronic cash."[77] Leaving aside counterfeiting, physical transactions—routine cash transactions, for instance—have never quite suffered from these acute problems of trust and assurance.[78] Yet for the reasons described above,[79] simple two-party exchanges of value over electronic networks could not occur prior to the blockchain innovation.

B. The Economic Properties of a Blockchain-Based Currency

This Section now explores the economic properties of a blockchain-based currency like bitcoin. It examines its basic economic qualities, as compared to commodity money (like gold) and fiat money (like banknotes). It summarizes the key arguments for and against a blockchain-based currency and concludes that, whatever one's normative views regarding the desirability of such a currency, the technology's distinctive features indisputably hold potential for the efficient transfer of all sorts of digital value.

Innovation and disruption in the "technology of money"[80] is not new;[81] this competitive landscape has existed for thousands of years.

74. *See* Kerem Kaşkaloğlu, *Near Zero Bitcoin Transaction Fees Cannot Last Forever*, INT'L CONF. ON DIGITAL SECURITY & FORENSICS 91, 91–93 (June 2014), http://sdiwc.us/digitlib/request.php?article=96cd6f6067fcbaf5e3947d071aa688fb [https://perma.cc/HAE4-CYU2] (arguing that zero or infinitesimal transaction fees will not be sustainable, given characteristics of mining, securing the network from dishonest users, and the scarce supply).

75. *See infra* notes 240–44 and accompanying text.

76. *See* NAKAMOTO, *supra* note 31, at 8 (concluding that the proposed system for electronic transactions works without relying on trust because it uses a public history of transactions, which makes it impractical for them to be changed later on).

77. *Id.* at 1.

78. "Show me the money," an in-person seller could say.

79. *See supra* notes 54–55 and accompanying text.

80. I use the term "technology of money" to refer to the idea that money, in whatever the currently accepted form may be, represents a particular society's "practical . . . use of scientific and mathematical discoveries." *See Technology*, BLACK'S LAW DICTIONARY (10th ed. 2014).

81. And neither are unregulated currencies. *See generally* DAVIES, *supra* note 40 (tracing

For any technology—be it gold, banknotes, or bitcoin—to be accepted as a monetary standard, it must perform three important functions especially well: it must be (1) a medium of exchange,[82] (2) a store of value,[83] and (3) a unit of account[84] (collectively the functions of money). When a new standard comes along that performs the functions of money better than the incumbents, a platform shift occurs, and the old standard is replaced.[85]

Once upon a time, commodities—shells, grain, and metals—operated as primitive monetary technologies.[86] Among these early prototypes, gold reigned supreme because, of all the naturally occurring elements, its physical properties made it most suitable to perform the functions of money.[87] Despite its first-mover advantage of more than 4000 years,[88] gold was eventually disrupted by the next

---

the development of money and currencies).

82. *See id.* at 13–18 (explaining that in the barter system, goods could not as easily be bought and sold because of valuation and exchange-rate problems). A good monetary platform provides users with liquidity and trade efficiency. In other words, it eliminates the problems that make a pure barter system inefficient. For example, say you have three chickens; all I have is a cow. I need one dozen eggs—a task for which my cow is obviously unfit. If my cow cannot produce anything you need, we are out of a deal. This problem is called the "double coincidence of wants." *Id.* at 15. Second, even if you decide you could use some milk, we are faced with the problems of valuation and exchange rate. *Id.* What is my cow's milk worth as to your chickens' eggs?

83. A good monetary platform provides users with wealth stability—safety, storage, and retrieval features, for example. N. GREGORY MANKIW, PRINCIPLES OF MACROECONOMICS 643 (5th ed. 2008).

84. A good monetary platform provides users with a standardized unit of measurement, meaning users can track the value of economic items such as assets, liabilities, income, and expenses. *Id*.

85. *See generally* George Selgin, *Adaptive Learning and the Transition to Fiat Money*, 113 ECON. J. 147, 162 (2003) (examining how the exchange medium effects influenced the development of money and when and how the transition from a barter to a money system occurs).

86. *See* DAVIES, *supra* note 40, at 35–45 (tracing the evolution of commodities used as primitive money).

87. It is dense, meaning a lot of value can be held in a little space; it is light enough to transport with relative ease; it does not corrode or decay; it is easily divisible into smaller pieces; and it is very hard to counterfeit. *Why Gold?*, NPR: PLANET MONEY (Nov. 16, 2010), http://www.npr.org/blogs/money/2011/02/07/131363098/the-tuesday-podcast-why-gold [http://perma.cc/A9QG-49C7].

88. Many historians claim the first coins containing gold were struck in Lydia, Asia Minor (modern-day Turkey), around 600 B.C. *See, e.g.*, DAVIES, *supra* note 40, at 61–65 (recounting the development of the first bimetallic coinage in Lydia); *see also generally* Robert A. Mundell, *The Birth of Coinage* (Columbia Univ. Dept. of Econ. Discussion Paper Series, Paper No. 0102-08, Feb. 2002) (tracing the development of coinage in the first millennium B.C. in Asia Minor and examining the evidence that they were invented in Lydia).

innovation in monetary technology, government-backed banknotes.[89] Though still a physical technology, banknotes offered streamlined features: portability, divisibility, storability, and fungibility.[90] Soon after, another fundamental shift—this time digital—in monetary technology occurred: electronic deposits and transfers.[91]

1. *Bitcoin's Downside: Blockchain-Based Currencies are a Poor Store of Value*. Gold and paper money have worked as monetary platforms because these technologies perform the functions of money especially well. Gold worked as a store of value due to its physical characteristics.[92] The move away from gold was brought on by the realization that commodity money ties a country's economy to a scarce natural resource, and this can have destabilizing effects.[93] In other words, when Mother Nature controls the supply, shocks can occur that are beyond control.[94] By contrast, fiat currency's supply—and thus its value—is protected by regulation.[95] It is the only platform

---

89. In 1870, the Supreme Court struck down the Legal Tender Act of 1862, 12 Stat. 345, the first legislation aimed at creating paper money under Article I of the Constitution. Hepburn v. Griswold, 75 U.S. (8 Wall.) 603, 624 (1870). The very next year, a new Court overturned this decision, reasoning that the Civil War was a crisis that necessitated Congress's power to declare paper money to be legal tender and that it was not forbidden by the Constitution. Knox v. Lee (Legal Tender Cases), 79 U.S. (12 Wall.) 457, 540–47 (1871) ("Whatever power there is over the currency is vested in Congress. If the power to declare what is money is not in Congress, it is annihilated."). Finally, the Court extended *Knox* to uphold the validity of legal-tender laws during peacetime in *Juilliard v. Greenman*, 110 U.S. 421, 450 (1884). Indeed, one court has gone so far as to declare, "Article I, section 8 of the United States Constitution clearly gives the United States Congress the power to make *anything it wishes* legal tender." Lowry v. State, 655 P.2d 780, 782 (Alaska Ct. App. 1982) (emphasis added). For an extended discussion, see generally JAMES WILLARD HURST, A LEGAL HISTORY OF MONEY IN THE UNITED STATES, 1774–1970 (1973).

90. *See* WILLIAM STANLEY JEVONS, MONEY AND THE MECHANISM OF EXCHANGE 30–31 (1875) (explaining the ideal properties in choosing the material of money, in particular portability and divisibility); SWANSON, *supra* note 37, at 12–13 (describing the differences in storability and portability, among other factors, between gold, banknotes, and bitcoin).

91. *See* DAVIES, *supra* note 40, at 649 (arguing that this innovation is second only to the printing of paper money in the history of monetary technology).

92. *See supra* note 87.

93. EDWARD B. BARBIER, SCARCITY AND FRONTIERS 238 (2011).

94. *See id*. The Panic of 1857, for example, was triggered when a hurricane off the coast of the Carolinas sunk the S.S. Central America, a vessel carrying thirty thousand pounds of gold. This sum represented the money supply of many East Coast banks. William J. Broad, *X Still Marks the Sunken Spot, and Gold Awaits*, N.Y. TIMES, May 4, 2014, at A1.

95. *See* DONALD R. WELLS, THE FEDERAL RESERVE SYSTEM: A HISTORY 19–20 (2004). Fiat systems rest on the generally accepted premise that a country's citizens are better off when their federal government controls the money supply. *Id*. at 195.

recognized as legal tender,[96] the government is obliged to accept it for tax payment,[97] the central bank has monopoly control over supply,[98] and it is often backed by indirect collateral[99] and insurance.[100] These characteristics allow greater price stability.[101] For example, the Federal Reserve can adjust supply to navigate macroeconomic and financial policy issues.[102]

On the issue of value, a blockchain-based currency such as bitcoin is an imperfect substitute for fiat currency in much the same way gold is. The mathematic rules governing the bitcoin mining process[103] are designed to mimic gold.[104] So just as the laws of nature govern the gold supply, the laws of math govern the bitcoin supply.[105] In both cases, supply cannot be adjusted "to deal with recessions or to counteract destabilizing periods of inflation or deflation."[106] This might explain why the market has experienced wild price volatility.[107]

---

96. *See* 31 U.S.C. § 5103 (2012) ("United States coins and currency . . . are legal tender for all debts, public charges, taxes, and dues. Foreign gold or silver coins are not legal tender for debts.").

97. *Id*.

98. *See* 12 U.S.C. § 411 (2012) (directing that Federal Reserve Notes are to be issued at the discretion of the Board of Governors of the Federal Reserve System).

99. *See* 12 C.F.R. § 9.10(b) (2012) (clarifying that acceptable collateral may be direct obligations or other obligations guaranteed by the United States as to principal and interest).

100. U.S. bank accounts are often insured by the Federal Deposit Insurance Corporation (FDIC). *See* 12 C.F.R. § 330.3 (2012) (explaining the general principles of the insurance coverage).

101. *See* WELLS, *supra* note 95, at 127, 190, 195. The Federal Reserve does this through a combination of lowering and stabilizing inflation, limiting fluctuation in the business cycle, and standing as a lender of last resort during periods of turmoil. *Id.*

102. *See id.* at 150 (discussing various normative perspectives on the Federal Reserve's proper role in setting monetary policy).

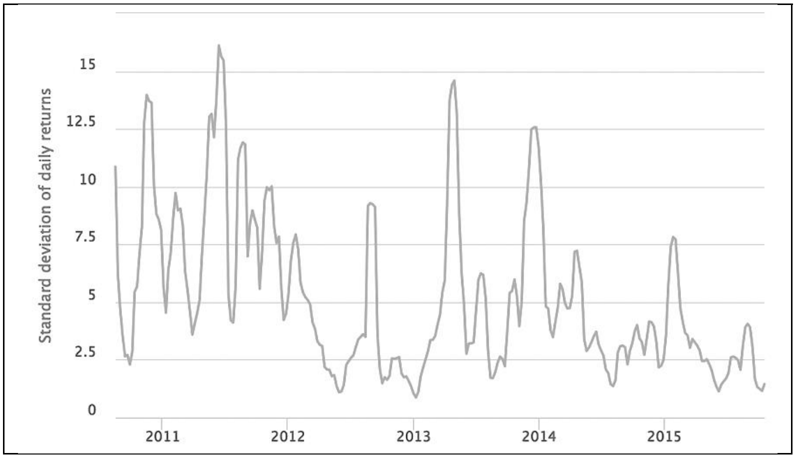
103. *See supra* notes 56–77 and accompanying text.

104. *See supra* notes 72–74 and accompanying text.

105. *See id.* This rule has one important caveat. Although initial distribution is fixed, its parameters can be altered through a majoritarian process. *An Interview with Eric Posner*, *in* 21 GOLDMAN SACHS GLOBAL MACRO RESEARCH 4, 5 (2014). Commentators find this unsettling because it means "technology and programming experts" wield control over a money supply, rather than "economists or monetary experts." *E.g.*, *id.* At least one commentator has explored the possibility of managing the money supply to create a stable blockchain-based currency without the need for intermediation at all. *See* Cameron Harwick, Cryptocurrency and the Problem of Intermediation 12–15 (May 31, 2015) (unpublished manuscript), http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2612727_code2326669.pdf?abstractid=2523771&mirid=1 [http://perma.cc/XZ9V-E72D]. However, since these parameters are fixed at the outset and bitcoin is very widely held, problems of coordination and collective action make it highly unlikely, as a practical matter, that any of the initial parameters will ever be altered.

106. David S. Evans, *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms* 7 (Coase-Sandor Institute Inst. for L. & Econ., Working Paper No. 685,

Figure 1. Bitcoin Volatility Time Series from Aug. 16, 2010 to Oct. 20, 2015.[108]



Over its history, bitcoin's exchange rate against the U.S. dollar has frequently jumped or crashed over 20 percent (sometimes nearly 50 percent) in the course of a single day.[109] By contrast, over the same period, the U.S. dollar-to-euro exchange rate has never changed more than 2.5 percent in one day.[110] Even a casual observer can recognize that such instability is not a desirable currency trait because its

2014), http://www.law.uchicago.edu/files/file/685-dse-economic.pdf [http://perma.cc/3NET-EYEB].

107. *See infra* Figure 1. Liquidity and pricing issues also exist. Bitcoin is a relatively illiquid asset. *See Illiquid asset*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining illiquid asset as "[a]n asset that is not readily convertible into cash, usu. because of (1) the lack of demand, (2) the absence of an established market, or (3) the substantial cost or time required for liquidation" (alteration in original)). Accordingly, relatively small trades can move these thin markets. 2 JOHN MAYNARD KEYNES, A TREATISE ON MONEY: THE APPLIED THEORY OF MONEY 67 (1930). And prices are different across different exchanges, indicating that some markets carry a liquidity premium—for example, ones that allow users to more readily convert their holdings to fiat. All bitcoin-to-fiat trades are liquidity trades because the asset lacks underlying fundamentals. To attract business, payment processors such as BitPay must guarantee the price for a period of time so businesses may accept bitcoin payments without the corresponding price risk. *See Bitcoin Exchange Rates*, BITPAY, https://bitpay.com/bitcoin-exchange-rates [https://perma.cc/4EUZ-YJH3] (listing the exchange rates).

108. THE BITCOIN VOLATILITY INDEX, https://btcvol.info [http://perma.cc/XTF5-4B3G]. Volatility in this figure is represented by the standard deviation of daily returns for the preceding thirty-day window over the past five years. *Id.*

109. Harwick, *supra* note 105, at 6.

110. *Id*.

holder's purchasing power can increase or decrease drastically and suddenly.[111]

2. *Bitcoin's Upside: A More Efficient Medium of Exchange*. Though the technology fails as a store of value for reasons described above, the blockchain could play an integral role in the next phase of the financial-technology (fintech) revolution. Given its features, it is a technology uniquely capable of performing several key components of a transaction—recordkeeping, auditing, monitoring, enforcement, or asset custody (that is, escrow)—in addition to facilitating the trade itself. This is important because the global movement of value can be quite cumbersome.[112]

For example, gold and fiat currency have always had high transportation costs, involving security, armored cars, and insurance.[113] In fact, the simple laws of physics limited the Federal Reserve's original structure; the number and locations of the Reserve Banks are such that "no bank [was] more than an overnight's train ride from its [Federal Reserve]."[114] These restraints were shattered by the first wave of the digital revolution, in which electronic transfers greatly reduced the cost of moving value.[115]

Yet the movement of value along these electronic systems is still costly. First, moving value—actually clearing and settling a transaction—takes time. For example, on January 26, 2015, the Federal Reserve issued a call to action for all stakeholders in the U.S.

---

111. For an extended discussion of bitcoin's volatility problem, see generally Mitsuru Iwamura, Yukinobu Kitamura, Tsutomu Matsumoto & Kenji Saito, *Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money* (Hitotsubashi Univ. Inst. of Econ. Research, Discussion Paper Series A No. 617, 2014) (suggesting an amendment to the Bitcoin protocol to set monetary policy without a central bank).

112. *See* DAVIES, *supra* note 40, at 596–602 (describing the "poverty trap" faced by many countries, despite the rapid increase of wealth in many others).

113. *See id.* at 606 (describing, for example, the prohibitive costs of transporting silver in rural Africa).

114. U.S. GEN. ACCOUNTING OFFICE, FEDERAL RESERVE SYSTEM: CURRENT AND FUTURE CHALLENGES REQUIRE SYSTEMWIDE ATTENTION 83 (1996).

115. As early as 1984, banks recognized that "[i]nformation about money" is "almost as important as money itself." Thomas A. Bass, *The Future of Money*, WIRED (Oct. 1996), http://archive.wired.com/wired/archive/4.10/wriston_pr.html [http://perma.cc/98R4-L9RQ]. Today, "[d]igitization is challenging the very way banks operate." Somesh Khanna, *The Bank of the Future*, MCKINSEY & CO. (Nov. 2014), http://www.mckinsey.com/insights/financial_services/the_bank_of_the_future [http://perma.cc/U8ST-J8XH].

payments system[116] to increase end-to-end payment speed, among other things.[117] Currently, the Automated Clearing House[118] (ACH) system supports more than 20 percent of all electronic payments in the United States—these transactions, to a great extent, relate to consumer and small-business transactions.[119] More than $40 trillion moves through the ACH network each year in nearly 23 billion electronic transactions.[120] Nearly all consumer transactions on the ACH network take two to three days.[121] Second, moving money takes money. For example, an estimated $600 billion in principal will be sent in the remittance[122] market in 2015.[123] Companies like Western Union and MoneyGram traditionally provide this service and enjoy an average fee (or "take rate") of 6 percent, though this rate can run as high as 9 percent.[124] This translates to roughly $36 billion in fees in 2015.

---

116. *See* FED. RESERVE SYS., STRATEGIES FOR IMPROVING THE U.S. PAYMENT SYSTEM 6–7 (2015), https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf [https://perma.cc/GL6W-PR4S] (calling all stakeholders to seize the opportunity of the current critical juncture and improve the U.S. payment system).

117. *Id.* at 7.

118. Created in 1974, ACH is an electronic network of U.S. financial institutions. It was designed to reduce the need for paper checks in making "routine payments." *Automated Clearing Houses (ACHs)*, FED. RESERVE BANK OF N.Y., http://www.ny.frb.org/aboutthefed/fedpoint/fed31.html [http://perma.cc/66MX-K3CK].

119. *History and Network Statistics*, NACHA—THE ELEC. PAYMENTS ASSOC., https://www.nacha.org/ach-network/timeline [https://perma.cc/5T2B-7KPE]. The other major electronic-value transfer systems, Fedwire and CHIPS—sometimes called "large-value payment systems"—are primarily used by financial institutions to settle large financial-market and other transactions. *See* COMM. ON PAYMENT & SETTLEMENT SYS., BANK FOR INT'L SETTLEMENTS, *Payment, Clearing and Settlement Systems in the United States*, *in* 2 PAYMENT, CLEARING AND SETTLEMENT SYSTEMS IN THE CPSS COUNTRIES 471, 487 (2012).

120. NACHA—THE ELEC. PAYMENTS ASSOC., ACH VOLUME INCREASES 5.3 PERCENT IN 1ST QUARTER 2015, at 1, https://www.nacha.org/system/files/resources/1st%20Quarter%202015.pdf [https://perma.cc/5533-CRZM].

121. Although transactions can technically clear overnight on the ACH network, they are generally subject to batch processing, a process whereby a large volume of transactions is aggregated for simultaneous movement through the network.

122. Remittances are money transfers by (typically foreign) workers to other individuals (typically relatives in their home country). *See Remittance*, WEBSTER'S UNABRIDGED DICTIONARY 1630 (2d ed. 2014) (defining the term as "money or its equivalent sent from one place to another").

123. Mark Scott, *Remittances at the Click of a Smartphone Button*, N.Y. TIMES: BITS (June 7, 2015, 9:00 AM), http://bits.blogs.nytimes.com/2015/06/07/remittances-at-the-click-of-a-smartphone-button [http://perma.cc/V6PG-2AZN] (citing a study by the World Bank).

124. DILIP RATHA ET AL., THE WORLD BANK, MIGRATION AND DEVELOPMENT BRIEF 23, at 12 (2014), http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationandDevelopmentBrief23.pdf [http://perma.cc/RS2L-58AM].

Blockchain technology is uniquely positioned to tackle the problems of both speed and cost. For example, Coinbase, a prominent bitcoin company, provides a service called Instant Exchange.[125] This service facilitates instantaneous cross-border money transfers with bitcoin as the intermediary for a total transaction cost of 2 percent.[126] As applied to the $600 billion principal figure above (today's remittance market), a potential cost savings of $24 billion might pass through directly to the consumers of such a service.[127]

For these reasons (and many more that are beyond the scope of this Note), the financial-services sector is in the midst of a digital revolution.[128] Of the $23.5 billion invested in fintech ventures between 2013 and 2014, 23 percent ($5.4 billion) was invested in payments technology.[129] As illustrated above, one critical aspect of payments technology is infrastructure. Payments-infrastructure initiatives are emerging in many countries across the world, driven by both public and private actors.[130] Many players—from bootstrapping startups to large, incumbent financial institutions—believe blockchain technology will play an integral role.[131]

In sum, blockchain technology solves an important problem in electronic value transfers. The blockchain does not only move value; it also integrates several components of the trading-clearing-settlement value chain in an elegant, efficient, and mathematical way.

---

125. *Instant Exchange*, COINBASE, https://www.coinbase.com/instant-exchange [http://perma.cc/D9DE-TFB6].

126. *What is Instant Exchange?*, COINBASE, https://support.coinbase.com/customer/portal/articles/2021569-what-is-instant-exchange [http://perma.cc/Z8TK-8RAR] (noting that Coinbase's standard 1 percent fee is applied on both sides of the transaction).

127. This amount is calculated as follows: First, solve for the difference between the average prevailing rate (that is, 6 percent) and Coinbase's low-cost position (that is, 2 percent) to arrive at 4 percent. Second, solve for 4 percent of the $600 billion principal figure. The amount is $24 billion.

128. *See* ACCENTURE, THE FUTURE OF FINTECH AND BANKING: DIGITALLY DISRUPTED OR REIMAGINED? 3 (2015), https://www.accenture.com/t20150707T195228__w__/lven/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Future-Fintech-Banking.pdf [https://perma.cc/3QL2-567B] (reporting a 201 percent increase in fintech investments from 2013 to 2014); *see also* MARIANO BELINKY, EMMET RENNICK & ANDREW VEITCH, THE FINTECH 2.0 PAPER: REBOOTING FINANCIAL SERVICES (2015), http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/jun/The_Fintech_2_0_Paper_Final_PV.pdf [http://perma.cc/9LMK-XQ4U] (discussing the significant changes in the policy and technology surrounding fintech).

129. BELINKY ET AL., *supra* note 128, at 4.

130. *See* Rob Hayden, *Transforming National Payments Systems*, 20 MCKINSEY ON PAYMENTS 23, 24 (Sept. 2014).

131. For articles on bank innovation around blockchain technology, see *supra* note 4.

To be sure, these facts neither imply nor foreclose on the desirability of a blockchain-based currency. They simply indicate that blockchain technology should be of interest to any industry engaged in the digital transfer of value. For example, instead of being used as an alternative currency, it might facilitate the transfer of traditional units of value—U.S. dollars or euros for example. In other words, incumbent firms in the payments-and-transfer space can co-opt it to gain efficiencies systems, lower fee structures, and provide more competitive services.[132]

II. THE DEVELOPING LEGAL FRAMEWORK FOR BLOCKCHAIN TRANSACTIONS

Part I explained how money has evolved over time, both as a technology and as a concept. Specifically, it has shifted from a store of value in itself to a medium of exchange. As the role of cash diminishes in favor of electronic deposits and transfers,[133] many wonder about the extent to which blockchain-based currencies will influence the next phase of this global payment revolution. Indeed, entrepreneurial ventures—some backed by considerable human and financial resources—are building a vibrant ecosystem of complementary products and services around this vision.[134] One view, hailing the virtues of a free, open currency market is that transactions in this space should be entirely deregulated.[135] This Part concludes at

---

132. One prominent example in this space is Ripple, a company that has designed a protocol similar to Bitcoin for routing payments and settling funds. Designed to simplify interbank payments at the infrastructure level, Ripple has end users in the financial industry, including banks, governments, and clearinghouses. RIPPLE, EXECUTIVE SUMMARY FOR FINANCIAL INSTITUTIONS 2 (2015), https://ripple.com/files/ripple_executive_summary.pdf [https://perma.cc/W83S-8XSF]. For a note on the technical distinction between Bitcoin and Ripple, see *infra* note 170. For a discussion on Ripple's recent settlement agreement with FinCEN, see *infra* notes 171–74 and accompanying text.

133. *See* DAVIES, *supra* note 40, at 649–52 (discussing the global move toward electronic transactions).

134. *See* Grinberg, *supra* note 27, at 165 ("A growing ecosystem surrounds Bitcoin, including exchanges, transaction services providers, market information and chart providers, escrow providers, joint mining operations and so on."); *see also* Michael A. Cusumano, *The Bitcoin Ecosystem*, COMM. OF THE ACM, Oct. 2014, at 22, https://www.deepdyve.com/lp/association-for-computing-machinery/the-bitcoin-ecosystem-fUAzCpWvpD [https://perma.cc/PE6T-NV6W] ("[B]itcoins are a complex platform technology that requires the help of intermediaries—an ecosystem of 'complementary' product and service providers that charge fees.").

135. *See* Nikolei M. Kaplanov, Comment, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 171 (2012) (arguing that "bitcoins should be treated as an unregulated community currency under the

the outset without further discussion that such a view is neither realistic nor desirable, given a compelling policy interest in preventing abuse and misuse.[136] Examples of such abuses include bitcoin's potential to facilitate black-market transactions,[137] tax evasion,[138] money laundering,[139] and terrorist financing.[140]

This Part explores the emerging legal framework around virtual currencies and serves as a practical guide for policymakers and innovators trying to both shape and navigate it. Both federal and state regulators have identified some basic risks around blockchain-based currencies and begun staking jurisdictional claims. Policymakers are currently revisiting complex, interwoven regulatory frameworks—primarily banking laws, commodities laws, and securities laws—to shoehorn the technology into existing frameworks and consider where new ones might be appropriate. This Part presents a patchwork that is continuing to emerge,[141] with special attention on areas posing uncertainty for innovators.

A. Federal Regulation of Blockchain-Based Currencies

No comprehensive federal regulation exists for virtual currencies. Many government bodies—specifically, FinCEN, the Internal Revenue Service (IRS), SEC, CFTC, and Consumer Financial Protection Bureau (CFPB)—have offered guidance and taken limited action. This Section summarizes the most significant federal developments to date—FinCEN's guidance, administrative rulings, and enforcement against Ripple Labs, Inc. (Ripple)[142]—and explains the likely implications for innovators. Finally, it notes the

---

law").

136. For a thoughtful discussion on normative and logistical issues in regulating Internet activity, see generally LAWRENCE LESSIG, CODE VERSION 2.0 (2d ed. 2006).

137. Ly, *supra* note 28, at 595 (discussing Silk Road).

138. *Id*. at 595–96.

139. *Id*. at 594.

140. *See* SWANSON, *supra* note 37, at 28 (mentioning terrorist financing and money laundering as two of the possible pitfalls of Bitcoin).

141. Given the fixed nature of print publication, readers should visit DAVIS POLK & WARDWELL LLP, *supra* note 39, for the latest developments on regulation of Bitcoin and other virtual currencies.

142. The IRS has also issued a notice declaring that virtual currencies should be treated as property for federal tax purposes. *See IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*, INTERNAL REVENUE SERV. (Mar. 25, 2014), http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance [http://perma.cc/3F4A-KHLA]. For an extended discussion of the implications of this rule for the bitcoin economy, see Ly, *supra* note 28, at 606–08.

limited scenarios in which the other agencies have jurisdiction over blockchain activities.

1. *FinCEN Guidance, Rulings, and Enforcement.* Under the Bank Secrecy Act (BSA),[143] banks and other financial institutions are subject to various registration and recordkeeping requirements.[144] All "money service businesses"[145] are required to register with the Department of the Treasury[146] and develop anti-money-laundering[147] and customer identification programs.[148] In March 2013, FinCEN[149] extended these rules to cover certain participants who transact in "convertible virtual currencies."[150] It defined this term to include any medium of exchange that "operates like a currency in some environments," and "has an equivalent value in [or acts as a substitute for] real currency," but does not have "legal tender status in any jurisdiction."[151]

Under FinCEN's guidance, "exchangers" and "administrators" are possibly subject to regulation.[152] Exchangers are persons or businesses that exchange virtual currency for real currency, funds, or other virtual currency.[153] Administrators are persons or businesses engaged in the business of "issuing (putting into circulation) a virtual currency" who also have "the authority to redeem (to withdraw from

143. Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (codified at 12 U.S.C. §§ 1829b, 1951–59 and 31 U.S.C. §§ 5311 et seq.).

144. Courtney J. Linn, *Redefining the Bank Secrecy Act: Currency Reporting and the Crime of Structuring*, 50 SANTA CLARA L. REV. 407, 412–20 (2010) (providing an overview of the registration and record-keeping requirements for banks and other "money transmitters").

145. The term "money services business" includes "money transmitters," defined as a person that accepts and transmits currency, funds, or other value that substitutes for currency. 31 C.F.R. § 1010.100(ff) (2015).

146. *Id.* § 1022.380(a).

147. *Id.* § 1022.210(a).

148. *Id.* § 1022.210(i).

149. Established in 1990, the Financial Crimes Enforcement Network, or FinCEN, is a bureau of the Department of the Treasury that combats domestic and international money laundering, terrorist financing, and other financial crimes. *What We Do*, FinCEN, http://www.fincen.gov/about_fincen/wwd/ [http://perma.cc/S72W-VBJE].

150. FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1 (2013), http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf [http://perma.cc/5XAF-PAFC] [hereinafter FINCEN GUIDANCE].

151. *Id.*

152. *Id.* at 2.

153. *Id.*

circulation) such virtual currency."[154] An exchanger or administrator becomes a "money transmitter" subject to these registration and recordkeeping requirements when they either "accept[] and transmit[]" convertible virtual currency or "buy[] or sell[]" convertible virtual currency.[155] "Users" are explicitly carved out.[156]

In 2014, FinCEN issued four rulings under this guidance[157] that, together with existing BSA laws, provide some key insights. First, any blockchain transaction is likely a virtual-currency transaction, because even nonfinancial uses require a de minimis amount of currency (that is, a fraction of a penny of bitcoin). However, such activity must also be performed by an "exchanger" or "administrator" to trigger BSA requirements.[158] End users, such as merchants or consumers, are likely to be exempted.[159]

Second, a user who mines virtual currency (miner-user) is not a money transmitter, even if he uses the bitcoin to purchase goods and services.[160] Further, miner-users converting virtual currencies to real or other virtual currencies are not subject to BSA requirements, so long as their conversion is for personal use.[161] Therefore, miner-users

---

154. *Id*.

155. *Id*. at 3.

156. "Users" are persons who obtain virtual currency "to purchase goods and services." *Id*. at 2.

157. FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2014-R001, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY MINING OPERATIONS (2014) [hereinafter FINCEN RULING 1], http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf [http://perma.cc/Q4PL-F92L]; FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2014-R002, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY SOFTWARE DEVELOPMENT AND CERTAIN INVESTMENT ACTIVITY (2014) [hereinafter FINCEN RULING 2], http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf [http://perma.cc/P8K4-WTQQ]; FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2014-R011, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL CURRENCY TRADING PLATFORM (2014) [hereinafter FINCEN RULING 3], http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf [http://perma.cc/HL78-LDHQ]; FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2014-R012, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL CURRENCY PAYMENT SYSTEM (2014) [hereinafter FINCEN RULING 4], http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf [http://perma.cc/NZA9-WLTR].

158. *See supra* text accompanying notes 152–55.

159. *See* FINCEN GUIDANCE, *supra* note 150, at 1 ("A user of virtual currency is *not* an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations.").

160. FINCEN RULING 1, *supra* note 157, at 3.

161. This conclusion is grounded in the "end user" exemption. *See supra*, note 159 and accompanying text. It is supported by FINCEN GUIDANCE. *See supra* note 157, at 3. ("What is

should not be seen as money transmitters subject to the BSA's registration and recordkeeping requirements unless they are selling bitcoin as a business.[162]

Third, a company that mines virtual currency (miner-company) is not a money transmitter in certain instances. Specifically, miner-companies are not money transmitters when convertible virtual currency is used (1) to pay for goods or services, (2) to pay debts previously incurred, (3) to make distributions to owners, (4) to purchase real or other virtual currency specifically for any of the previous three purposes, or (5) for the company's own investment account.[163]

Fourth, a company is an "exchanger" regardless of whether it acts as a broker (by matching two simultaneous, offsetting transactions) or as a dealer (by transacting on its own account).[164] At least three U.S.-based exchanges have shut down in the wake of this guidance.[165]

Finally, two important exemptions (that predate both the guidance and the rulings) carve out certain activities from the definition of money transmitter: the "integral" exemption and the

---

material to the conclusion . . . is not the mechanism by which person obtains the convertible virtual currency, but what the person uses the convertible virtual currency for, and for whose benefit.").

162. FINCEN GUIDANCE, *supra* note 150, at 2 & n.7.

163. FINCEN RULING 1, *supra* note 157, at 3; FINCEN RULING 2, *supra* note 157, at 4.

164. FINCEN RULING 3, *supra* note 157, at 3; FINCEN RULING 4, *supra* note 157, at 3.

165. Jon Matonis, *Fincen's New Regulations are Choking Bitcoin Entrepreneurs*, AM. BANKER: THE MONETARY FUTURE (Apr. 25, 2013), http://www.americanbanker.com/bankthink/fincen-regulations-choking-bitcoin-entrepreneurs-1058606-1.html [http://perma.cc/5ADR-M5FH]. The force of these regulations is compounded by the fact that, a few months after the FinCEN issued its guidance, the Office of the Comptroller of the Currency (OCC) issued guidance effectively raising the cost for banks and other financial institutions for conducting business with any blockchain-based currency companies. OCC Bulletin 2013–29, Third-Party Relationships: Risk Management Guidance (Oct. 30, 2013). To be sure, the guidance does not specifically address bitcoin or blockchain-based currencies; however, it refers to certain third-party relationships that involve "critical activities" and merit enhanced risk measures. *Id.* Specifically, the guidance requires the adoption of "risk-based processes" for third-party relationships commensurate with the level of risk and complexity inherent in those relationships. *Id.* With bitcoin businesses considered high risk due to their potential for money laundering and other illicit uses, this guidance means banks will have to conduct enhanced due diligence on any blockchain-based company. *Id.* Accordingly, many U.S. companies and entrepreneurs have had trouble accessing basic banking services. *See* Kashmir Hill, *Bitcoin Companies and Entrepreneurs Can't Get Bank Accounts*, FORBES (Nov. 15, 2013, 3:23 PM), http://www.forbes.com/sites/kashmirhill/2013/11/15/bitcoin-companies-and-entrepreneurs-cant-get-bank-accounts [http://perma.cc/CY76-ADVY] (reporting on the U.S.-based bitcoin exchanges that have shut down).

"payment processor" exemption. First, BSA legislation provides an exemption for entities that accept and transmit funds "only integral to the [entity's] sale of goods or the provision of [other, nonmoney transmission] services."[166] In other words, ordinary merchants and service providers who merely accept bitcoin as a convenience to customers are not money transmitters. Second, BSA legislation provides an exemption for any entity acting as a "payment processor to facilitate the purchase of . . . a good or service through a clearance and settlement system by agreement with the creditor or seller."[167] One condition necessary for this exemption is that the entities operate only through clearance and settlement systems that admit BSA-regulated financial institutions.[168] Accordingly, bitcoin-based payment processors will have a difficult time availing themselves of this exception because the virtual-currency leg of the transaction will always settle on the blockchain[169]—a system that inherently allows participation by non-BSA-regulated members.[170]

On May 5, 2015, in its first civil enforcement action against a virtual-currency business, FinCEN announced a $700,000 fine against

---

166. 31 C.F.R. § 1010.100(ff)(5)(ii)(F) (2015). FinCEN has specified a three-prong test for this exemption: (1) the money-transmission component must be part of the provision of goods or services distinct from money transmission itself, (2) the exemption can only be claimed by the person that is engaged in the provision of goods or services distinct from money transmission, and (3) the money transmission component must be necessary for the provision of the goods and services. FINCEN RULING 3, *supra* note 157, at 4; FINCEN RULING 4, *supra* note 157, at 4.

167. 31 C.F.R. § 1010.100(ff)(5)(ii)(B) (2015).

168. FinCEN has specified a four-prong test for this exemption: (1) the entity providing the service must facilitate the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself), (2) the entity must operate through clearance-and-settlement systems that admit only financial institutions regulated under the BSA, (3) the entity must provide the service pursuant to a formal agreement, and (4) the entity's agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds. FINCEN RULING 3, *supra* note 157, at 4–5; FINCEN RULING 4, *supra* note 157, at 4.

169. *See supra* Part I.A.

170. This exemption implicates an important distinction between "permissionless" networks (like Bitcoin) and "permissioned" networks (like Ripple). A permissionless network, such as the Bitcoin blockchain, is fully decentralized—in other words, participants may join the network, process transactions, and fully participate without any previous relationship with the ledger. *See* TIM SWANSON, CONSENSUS-AS-A-SERVICE: A BRIEF REPORT ON THE EMERGENCE OF PERMISSIONED, DISTRIBUTED LEDGER SYSTEMS 5 (2015), http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf [http://perma.cc/A2GA-SUQH]. Such a network will never meet the "payment processor" exemption because non-BSA-regulated entities cannot be screened out. By contrast, on permissioned networks, participants are whitelisted through some type of know-your-customer procedure. *Id.* Such a network may be designed to accommodate regulatory exemptions of this nature.

Ripple and a simultaneous settlement agreement.[171] Ripple was selling XRP, a virtual currency similar to bitcoin, that it designed for the purpose of creating a real-time settlement infrastructure.[172] In its negotiated settlement with the U.S. Attorney's Office in the Northern District of California, Ripple admitted to violating several BSA requirements in its "exchange" and "transmission" of XRP for fiat currency.[173] Though Ripple had registered its subsidiary as a money-services business in accordance with FinCEN's guidance, it sold XRP for several months without a proper anti-money-laundering (AML) program in place, failed to designate a compliance officer, and did not solicit an independent review of its practices and procedures.[174]

Two lessons can be learned from FinCEN's enforcement against Ripple. First, FinCEN is clearly taking a hard stance, per its 2013 guidance, that AML programs are a necessity from the very moment a business begins "exchang[ing]" or "transmi[tting]" customer funds.[175] Second, distributed-ledger businesses that operate outside of the traditional Bitcoin blockchain will not escape FinCEN's scrutiny.

2. *CFTC Jurisdiction over Bitcoin Derivatives and Market Manipulation Oversight*. As noted above,[176] blockchain-based currencies share some economic properties with commodity money,[177] and legal definitions support their characterization as a commodity in some instances. The Commodity Exchange Act (CEA)[178] broadly defines a "commodity" to include "all services, rights and interests . . . in which contracts for future delivery are presently or in the future

171. Press Release, Fin. Crimes Enf't Network, U.S. Dep't of the Treasury, FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger (May 5, 2015), http://www.fincen.gov/news_room/nr/pdf/20150505.pdf [http://perma.cc/T6WU-55Z4].

172. Does this sound familiar? *See supra* Part I.B.2.

173. U.S. DEP'T OF JUSTICE, SETTLEMENT AGREEMENT WITH RIPPLE LABS, INC., at app. A 4–6 (May 5, 2015), http://www.justice.gov/file/421626/download [http://perma.cc/DPD5-P8Q9].

174. *Id.* at app. A 5–6.

175. *See supra* text accompanying notes 152–56 (discussing exchangers and transmitters).

176. *See supra* Part I.B.1.

177. Indeed, one monetary economist established the term "synthetic commodity money" to describe the unique economic properties of a blockchain-based currency, such as bitcoin. *See* George Selgin, Synthetic Commodity Money 7–8 (Apr. 10, 2013) (unpublished manuscript), http://ssrn.com/abstract=2000118 [http://perma.cc/G2GY-BSNH].

178. Commodity Futures Trading Commission Act of 1974, Pub. L. No. 93-463, 88 Stat. 1389, 1395 (codified as amended at 7 U.S.C. §§ 1 et seq.) (defining the term "commodity" and providing for CFTC jurisdiction over all options and futures trading in commodities); *see also* William L. Stein, *The Exchange-Trading Requirement of the Commodity Exchange Act*, 41 VAND. L. REV. 473, 485–86 (1988) (discussing the meaning of "commodity" under the CEA).

dealt in."[179] Accordingly, the CFTC has jurisdiction over derivatives contracts[180] related to interests not traditionally thought of as commodities—Treasury securities, stock-market indices, and currencies, for example. Under this analysis,[181] the CFTC concluded that bitcoin and other virtual currencies are "properly defined as commodities."[182] And in September 2014, the agency oversaw the launch of the first bitcoin swap execution facility (SEF).[183]

Bitcoin derivatives—for example, a swap contract pegged to the U.S.-dollar-bitcoin exchange rate—are exotic instruments at this stage.[184] The more pressing question, then, is the extent to which the

179. 7 U.S.C. § 1a(9) (2012); *see also* 17 C.F.R. § 1.3 (2015) (codifying CFTC Final Rule 1.3(e)).

180. Derivatives contracts are agreements between two parties, the value of which is determined by the price of something else, such as a changing interest rate, financial index, or market price. *See generally* ROBERT L. MCDONALD, DERIVATIVES MARKETS 1 (2d ed. 2006) ("Derivatives [contracts] can be thought of as bets on the price of something.").

181. More accurately, it was a legal conclusion lacking any analysis. It can only be assumed, however, that analysis was driving the conclusion, and this analysis would be a proper line of reasoning if the CFTC's position is challenged. Indeed, CFTC Chairman Timothy Massad has used similar reasoning in contending that "[d]erivative contracts based on a virtual currency represent one area within [the CFTC's] responsibility." *Testimony of Chairman Timothy Massad Before the U.S. Senate Committee on Agriculture, Nutrition & Forestry*, U.S. COMMODITY FUTURES TRADING COMM'N (Dec. 10, 2014), http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6 [http://perma.cc/9LNA-NQVM].

182. Coinflip, Inc., Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the Commodity Exchange Act, Making Findings and Imposing Remedial Sanctions at 3, CFTC Docket No. 15-29 (Sept. 17, 2015), http://www.cftc.gov/idc/groups/public/@lrenforcement actions/documents/legalpleading/enfcoinfliprorder09172015.pdf [http://perma.cc/5B4W-PJ3G].

183. *See* Press Release, TeraExchange, TeraExchange Launches First Regulated Bitcoin Derivatives Trading (Sept. 12, 2014), http://www.teraexchange.com/news/2014_09_12_Launches%20First%20Regulated%20Bitcoin%20Derivatives.pdf [http://perma.cc/B3DG-3ACQ] (announcing the first regulated trading platform for bitcoin derivatives). An SEF is a type of regulated marketplace under Title VII of the Dodd-Frank Wall Street Reform and Consumer Protection Act. Specifically, it is a platform for swap trading that provides pretrade information—a spot-market index, bids, and offers—and an execution mechanism for swap transactions. *See* 7 U.S.C. § 1a(50) (2012) (defining "swap execution facility"). Swaps are agreements for parties to exchange cash flows over time, with one party paying the other based on the actual price in reference to the contractually specified price. MCDONALD, *supra* note 180, at 247. The first recorded swap in this space involved the sale of a multimillion-dollar Stradivarius violin to a wealth-management company. The buyer wanted to use bitcoins in consideration for the purchase, but the seller was worried about exchange-rate risk over the period of the contract, given wild price fluctuations. TeraExchange worked with the buyer to structure a deal that would protect both parties from losses, and it became the prototype for this SEF. *See* Paul Vigna & Michael J. Casey, *BitBeat: Bitcoin, Stradivarius Make Beautiful Music Together*, WALL ST. J.: MONEY BEAT (Mar. 28, 2014, 7:26 PM), http://blogs.wsj.com/moneybeat/2014/03/28/bitbeat-bitcoin-stradivarius-make-beautiful-music-together [http://perma.cc/A728-RC4D].

184. Currently, payment processors assume the exchange-rate risk from merchants. For

CFTC can exercise jurisdiction over spot-market transactions[185] under its anti-manipulation authority.[186] In other words, the CFTC has enforcement authority over spot transactions in certain instances because spot-market manipulation can affect derivatives market prices.[187] Thus, in certain cases the CFTC may regulate bitcoin pursuant to its anti-manipulation rules.[188] While manipulation oversight would bring some regulation to the spot market, one issue is whether manipulation oversight alone is sufficient, even under the broad anti-manipulation rules of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).[189]

Dodd-Frank extended the CEA's anti-manipulation rules to cover swaps and clarified that "manipulation" under the CEA includes not only "actual manipulation"[190] but also an intent-based "attempted manipulation."[191] This new authority was first exercised in

---

example, merchants typically utilize a payment-processing service, such as BitPay, to convert bitcoin-denominated payments to fiat currency almost immediately. *See Getting Started: Accepting Bitcoin Payment*, BITPAY, https://bitpay.com/docs [https://perma.cc/KHB2-UY6X]. One way payment processors may consider hedging this risk would be through derivatives.

185. A "spot transaction" is simply the current sale or purchase for immediate settlement. *Spot transaction*, BLACK'S LAW DICTIONARY (10th ed. 2014).

186. The CEA makes it a felony "to manipulate or attempt to manipulate the price of . . . any commodity." 7 U.S.C. § 9 (2012). The CEA also creates a private right of action to accompany the government's civil and criminal enforcement capabilities. *Id*. § 22(a); *see also id*. § 25(a)(1) ("Any person . . . who violates this chapter or who willfully aids . . . a violation of this chapter shall be liable for actual damages resulting from . . . such violation."). The exact meaning of "manipulation" has been debated, as is not statutorily defined. Broadly stated, manipulation is an intentional exaction of a price determined by forces other than supply and demand.

187. *See* Jerry W. Markham, *Manipulation of Commodity Futures Prices—The Unprosecutable Crime*, 8 YALE J. REG. 281, 283 (1991) (describing "market power manipulation"); *see also* JOSEPH M. BURNS, A TREATISE ON MARKETS: SPOTS, FUTURES, AND OPTIONS 93–94 (1979) (describing the CFTC's "preventive and punitive approaches for dealing with temporary monopolies").

188. *See* 7 U.S.C. § 9(3) (2012) ("In addition to the prohibition in paragraph (1), it shall be unlawful for any person, directly or indirectly, to manipulate or attempt to manipulate the price of any swap, or of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity.").

189. Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, tit. VII, 124 Stat. 1376, 1641–1802 (2010). Section 753 of Dodd-Frank amends section 6(c) of the CEA (codified at 7 U.S.C. §§ 9, 15 (2012)).

190. Before Dodd-Frank, "manipulation" generally required "actual manipulation," proven by a well-established four-prong test: (1) the ability to influence market prices, (2) the intent to create or affect prices not reflecting legitimate forces of supply and demand, (3) the existence of artificial prices, and (4) the accused caused such artificial prices. 2 THOMAS A. RUSSO, REGULATION OF THE COMMODITIES FUTURE AND OPTIONS MARKETS § 12.11 (1983).

191. 7 U.S.C. § 9(3) (2012) ("It shall be unlawful for any person, directly or indirectly, to

CFTC v. Atlantic Bullion & Coin, Inc.[192] In *Atlantic Bullion*, the CFTC brought a civil action against the coordinators of a Ponzi scheme involving spot-market silver contracts.[193] Over an eleven-year period, the defendants fraudulently sold silver contracts in a nationwide scheme.[194] The defendants never supplied any silver; instead, they misappropriated all the funds and issued false account statements.[195] Under a similar analysis, the CFTC could bring investor-protection measures to the spot market for blockchain-based currencies and derivative products.[196]

B. State Regulation of Blockchain-based Currencies

On June 3, 2015, New York's Department of Financial Services issued its final "BitLicense" framework for regulating "virtual currency businesses."[197] Over a period of almost one year, BitLicense went from its initial proposal[198] to reproposal[199] to final rule. The process gave rise to two comment periods that elicited thousands of letters[200] expressing a wide range of opinions. And although it is too

manipulate or attempt to manipulate the price of any swap, or of any commodity."). The CFTC implemented this provision in Final Rule 180.2. 17 C.F.R. § 180.1 (2012).

192. U.S. Commodity Futures Trading Comm'n v. Atl. Bullion & Coin, Inc., [2012–2013 Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 32,551 (D.S.C. June 6, 2012).

193. Complaint at 1, *Alt. Bullion & Coin, Inc.*, No. 8:12-cv-01503-JMC.

194. *Id*.

195. *Id*. at 2.

196. Similarly, investors have at least some protection under U.S. securities laws, to the extent they are dealing in interests in bitcoin-related investment vehicles. *See* SEC v. Shavers, No. 4:13-CV-416, 2014 WL 4652121, at *6 (E.D. Tex. Sept. 18, 2014) (finding an interest in a bitcoin-based Ponzi scheme to be an "investment contract" for purposes of U.S. securities laws and imposing civil monetary penalties under the Securities Act). For an extended analysis of market manipulation at the infamous and ill-fated Mt. Gox exchange, see *The Willy Report: Proof of Massive Fraudulent Trading Activity at Mt. Gox, and How it has Affected the Price of Bitcoin,* THE WILLY REP. (May 25, 2014), https://willyreport.wordpress.com/2014/05/25/the-willy-report-proof-of-massive-fraudulent-trading-activity-at-mt-gox-and-how-it-has-affected-the-price-of-bitcoin [http://perma.cc/N59G-BSMC].

197. N.Y. COMP. CODES R. & REGS. tit. 23, § 200 (2015).

198. N.Y. Dep't of Fin. Servs., Notice of Proposed Rulemaking on the Regulation of the Conduct of Virtual Currency Businesses, 36 N.Y. Reg. 14 (July 23, 2014) [hereinafter BitLicense Proposal]. The full text of the BitLicense Proposal is available from the NYDFS's website at http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf [http://perma.cc/38SU-8XDB].

199. N.Y. Dep't of Fin. Servs., Notice of Proposed Rulemaking on the Regulation of the Conduct of Virtual Currency Businesses, 37 N.Y. Reg. 8 (Feb. 25, 2015) [hereinafter BitLicense Reproposal]. The full text of the BitLicense Reproposal is available at http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf [http://perma.cc/VR2p-KCCU].

200. Nearly 4,000 comments were received over the course of this eleven-month period. *See Comments Regarding the Proposed Virtual Currency Regulatory Framework*, N.Y. DEP'T OF

early to draw any empirical conclusions on BitLicense's long-term market impact,[201] it has certainly raised the cost of entry for certain participants and will likely pave a smoother path to integration with the established banking system.

New York's regime covers most business activities[202] involving (1) "virtual currencies," defined to include decentralized blockchain-based currencies,[203] and (2) New York or New York customers.[204] Much of the uncertainty around BitLicense lurks in its protracted definition of "virtual currency business activities," which breaks down into five major prongs: (1) transmitting virtual currency; (2) holding virtual currency on behalf of others; (3) buying and selling virtual currency as a customer business; (4) providing exchange services as a customer business; and (5) controlling, administering, or issuing virtual currency.[205]

First, the "transmission" prong presents some uncertainty in the statutory language itself. For example, the definition includes "the transfer, by or through a third party, of Virtual Currency from a Person to a Person."[206] Imagine a business that simply transfers virtual

---

FIN. SERVS., http://www.dfs.ny.gov/legal/vcrf_comments.htm [http://perma.cc/J7H3-KANH] (collecting comments).

201. The application deadline passed only four months prior to this Note's publication. *See BitLicense Frequently Asked Questions*, N.Y. DEP'T OF FIN. SERVS., http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework_faq.htm [http://perma.cc/972V-5Q3A] ("[A]pplicants must apply by August 10, 2015.").

202. Exemptions are provided for approved exchange service providers chartered under New York Banking Law and mere merchant/consumer activities. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.03(c) (2015).

203. *Id.* § 200.02(m). This includes:

> Any type of digital unit used as a medium of exchange or form of digitally stored value [and is] broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort.

DAVIS POLK & WARDWELL LLP, NEW YORK'S FINAL "BITLICENSE" RULE: OVERVIEW AND CHANGES FROM JULY 2014 PROPOSAL 9 (2015), http://www.davispolk.com/sites/default/files/2015-06-05_New_Yorks_Final_BitLicense_Rule.pdf [http://perma.cc/V5KG-C9ZJ]. It does not include digital units that are used (i) solely within online-gaming platforms, such as Nintendo Wii Points; (ii) in connection with a customer-affinity or rewards program, such as Delta SkyMiles; or (iii) used as part of fiat prepaid cards. *Id.*

204. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.02(n) (2015). The extent of New York jurisdiction is very broad. It likely includes businesses that serve or solicit New York customers through web-based services when such businesses do not take adequate precautions to exclude such customers. However, because no prohibition precludes dividend distributions, businesses may choose to limit New York–facing activity to limited-purpose subsidiaries.

205. *Id.* § 200.02(q)(1)–(5).

206. *Id.* § 200.02(o).

currency internally between proprietary accounts. In such a case, the transmission prong rightly is not triggered because the business does not interact with any third parties. However, what if that same business also transfers virtual currency to third parties, but not for goods or services—for example, to pay dividend distributions or salaries? The statutory language does not resolve whether the business, by virtue of that fact alone, must carry a BitLicense.

Another wrinkle in the "transmission" prong is the explicit exception for transactions "undertaken for non-financial purposes" that do not involve "more than a nominal amount" of virtual currency.[207] "Non-financial" is not a statutorily defined term. Blockchain technology can be used in a number of ways that are clearly "non-financial"—for example, to facilitate identity verification,[208] digital-document verification,[209] or peer-to-peer transfers of digital assets.[210] In other cases, however, it is less clear whether this exception applies. For example, how would a smart contract[211] transferring a right to payment from financial assets using a nominal amount of virtual currency be treated?

Second, the "holding" prong presents uncertainty with respect to its scope. Though the draft language includes the word "securing," that word is absent from the final rule.[212] "Securing" virtual currency likely refers to multi-signature ("multi-sig") transactions. Multi-sig transactions involve more than two parties.[213] For example, a two-of-three multi-sig transaction is a transaction between three parties that requires the approval of two parties prior to settlement.[214] One implication of this feature is cryptographic escrow. For example,

207. Importantly, based on the structure of the rule itself, this is an exception from the "transmission" prong, not from the entire rule. *See id.* § 200.02(q)(1) (exempting this transaction from the definition of transmission).

208. *See, e.g.*, ONENAME, https://onename.com [https://perma.cc/9YZV-G5NK] (allowing users to sign their blockchain transactions with a verifiable personal identity).

209. *See, e.g.*, BLOCK NOTARY, http://www.blocknotary.com [http://perma.cc/KD26-F2F2] (allowing users to securely and digitally sign documents via blockchain transactions, performing a notary-like function).

210. For more examples of potential innovative applications of blockchain technology, see *infra* Part III.

211. For a discussion of smart contracts, see *infra* Part III.B.

212. *Compare* BitLicense Proposal, *supra* note 198, § 200.2(n)(2) (defining "Virtual Currency Business Activity" to include "securing . . . Virtual Currency on behalf of others), *with* N.Y. COMP. CODES R. & REGS. tit. 23, § 200.2(q) (2015) (omitting the word "securing").

213. ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES 129 (2014).

214. *Id.* at 129–30.

Party A and Party B enter a contract with payment provisions contingent on an objectively verifiable event. They enlist Party M as a mediator who will sign the transaction in favor of the appropriate party upon the occurrence or nonoccurrence of such event. Removing Party M from the scope of this prong is probably appropriate because Party M never actually takes custody of the assets.

Third, the "buying and selling" prong presents uncertainty in the statutory language. Specifically, this prong is triggered by the buying and selling of virtual currency "as a customer business"[215]—a phrase that, read broadly, could likely encompass a wide range of activity. The best way to view this prong seems to be that it refers to buying virtual currency from customers and selling virtual currency to customers on a principal or agency basis. Under this interpretation, sales of virtual currency to third parties that are not part of the customer-facing business should fall beyond the provision's scope.

Both the fourth and fifth prongs (that is, the "exchange services" and "controlling or administering" prongs) overlap with FinCEN's definitions of "exchangers" and "administrators" under FinCEN's 2013 guidance.[216] Likewise, the same analysis that applies under FinCEN's 2013 guidance would apply to covered activities under both prongs.[217] Miners and creators of decentralized virtual currencies likely would be excluded under the same reasoning, assuming their activities extend no further.[218]

Lastly, two exemptions are worth noting.[219] First, the "merchant/consumer" exemption is fairly straightforward. Like FinCEN's 2013 guidance,[220] it carves out merchants or consumers who use virtual currency solely for purchasing or selling goods or services, or solely for investment purposes. Second, a more ambiguous "software developer" exemption applies to individuals and businesses that engage solely in the development and dissemination of

215. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.2(q)(3) (2015).

216. *See supra* notes 152–56 and accompanying text.

217. *See supra* notes 160–63 and accompanying text.

218. *Id.*

219. The "non-financial purposes" exception to the "transmission" prong would not be considered an exemption here because it only operates as an exclusion to that specific element of "virtual currency business activity." *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 200.2(q)(1) (2015) (excluding non-financial purposes from this definition). In other words, a business may satisfy the "non-financial purposes" exception yet still be subject to the rule by means of one of the other four prongs.

220. *See supra* note 156 and accompanying text.

software.[221] NYDFS has consistently asserted that it is regulating financial intermediaries, not software developers.[222] However, the line between the two may not always be clear.

Consider a business that develops wallet software—mobile applications that allow users to view and manage their virtual-currency balance.[223] On one hand, the developer does not take custody of the user's virtual currency at any point, and it does not transmit or exchange virtual currency.[224] Instead, it simply provides the user with a blockchain access point. On the other hand, the software stores the user's private key—the secret mathematical code necessary for the user to access his holdings on the blockchain. This weighs against the exemption's application, because access to a user's private key is the functional equivalent of access to the user's holdings tied to that key. Accordingly, a security compromise in the wallet software could cause users to lose all or part of their virtual-currency holdings.[225]

In light of the prior analysis, it seems fair to say that the law will have at least two short-term consequences. First, it will raise the cost of entry for market participants by mandating various programs—cybersecurity,[226] consumer protection,[227] financial reporting,[228] and AML.[229] Indeed, many businesses have already chosen to exit New

---

221. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.02(q) (2015).

222. *See, e.g.*, *NYDFS Announces Final Bitlicense Framework for Regulating Digital Currency Firms*, N.Y. DEP'T OF FIN. SERVS. (June 3, 2015), http://www.dfs.ny.gov/about/speeches/sp1506031.htm [http://perma.cc/9Y8C-3BYS] ("[W]e have no intention of being a regulator of software developers—only financial intermediaries.").

223. *See Some Bitcoin Words You Might Hear: Wallet,* BITCOIN.ORG, https://bitcoin.org/en/vocabulary#wallet [https://perma.cc/SS6R-9MNC] (defining "wallet").

224. This assumes the service is purely a wallet provider and does not provide additional value-added services, such as an exchange of U.S. dollars to virtual currency.

225. *See, e.g.*, McMillan, *supra* note 8 (reporting on a digital attack in which $1.2 million in bitcoins were stolen from online virtual wallets).

226. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.16 (2015). Cybersecurity requirements would include board-approved cybersecurity policy and a program to protect electronic systems and sensitive data, qualified chief information security officer, annual reports to NYDFS, annual penetration testing and audits, and maintenance of a business-continuity and disaster-recovery plan, to be independently tested annually. *Id.* § 200.16(b); *id.* § 200.17.

227. *Id.* § 200.19. Consumer-protection requirements include the disclosure of material risks, including certain minimum disclosures: virtual currency is not legal tender, transactions are generally irreversible, and the risk of fraud, cyberattack, and total loss of value, among other risks. *Id*.

228. *Id.* § 200.14. Reports and financial disclosures

229. *Id.* § 200.15. AML requirements include initial and annual risk assessments, ten-year records of all transactions, suspicious activity reports, a customer identification program, Office

York, citing total compliance implementation costs between $50,000 and $100,000.[230] Second, the certainty of licensure decreases legal risk of companies operating in this space, so a smoother path will likely emerge for blockchain businesses to integrate with the established banking system.

III. THE BLOCKCHAIN REVISITED: THE SHAPE OF TRANSACTIONS TO COME

This Part builds on the explanation of blockchain technology set forth in Part I and illustrates why regulations designed to "broadly construe[]"[231] the definition of "virtual currency" may unintentionally engulf an entire realm of activities. First, it explains the concepts of "scripting" and "sidechains"[232]—innovations that could spawn additional applications for blockchain technology. Second, it surveys current research and experimentation at the cutting edge of cryptography and computer science that could impact commerce and on a similar order of magnitude as the Internet did. It closes by circling back to themes raised in Part II, exploring the challenge that regulators face as they seek to understand this technology.

A. The Blockchain Revisited: Scripting and Sidechains

Potential applications of blockchain technology are not limited to money transfers and payments. At its core, this protocol facilitates more than the exchange of "bitcoins"; it facilitates the exchange of *value*.[233] Part I established a series of important mathematical rules

---

of Foreign Asset Control (OFAC) checks and compliance, annual internal or external audits, and no structuring to evade reporting, or obfuscating identity. *Id*.

230. Daniel Roberts, *Behind the "Exodus" of Bitcoin Startups from New York*, FORTUNE (Aug. 14, 2015, 11:19 AM), http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense [http://perma.cc/T3WF-QEHE] (citing at least ten companies that chose to exit New York, rather than incur the costs of compliance).

231. *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 200.2(p) (2015) ("Virtual Currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort.").

232. *See* BACK ET AL., *supra* note 33, at 5 (introducing the term "sidechain," and describing it as a blockchain that is interoperable with the main Bitcoin blockchain).

233. *Id.* at 4 ("There are assets besides currencies that may be traded on blockchains, such as IOUs and other contracts, as well as smart property."); Evans, *supra* note 106, at 1 (defining the blockchain as a "protocol for sending, receiving, and recording value securely"); *see also infra* Part III.B (describing some alternative applications of blockchain technology); *see generally* SWANSON, *supra* note 37 (discussing ways in which blockchain technology can be utilized to exchange things of value).

that govern the network. Fundamentally, transactions have a three-part structure: (1) Party A sends a message to the network declaring the transaction; (2) Party B accepts the transaction by broadcasting its acceptance; and (3) the network participants verify the transaction's authenticity.[234] To be sure, this basic structure was designed for transferring ownership of bitcoins. But when people send and receive bitcoins, those bitcoins are best thought of as containers for value.[235] Like a digital envelope, these containers can carry "coins" across the network; but they can also transmit richer forms of information, holding promise for many compelling applications beyond bitcoin.[236]

A typical transaction follows a simple script—a set of instructions—that adheres to the three-part structure described above.[237] If the script were amended to contain additional conditions, users could engage in more sophisticated transactions. For instance, consider that Party A and Party B may want to add a fourth condition to that script structure: they only want the transaction to occur at a certain time, or upon the occurrence or nonoccurrence of a conditional event. Many possibilities branch out from this basic idea, and it has sparked much discussion around "smart" contracts.[238]

As a practical matter, developers cannot currently implement scripts like this in bitcoin transactions because protocol amendments require a majority consensus.[239] Similar to a corporate charter, default rules are easy to establish at the outset and much harder to change later on. This fact, paired with the open-source nature of the Bitcoin platform, has inspired dozens of "altcoins," or alternative-utility iterations on blockchain technology.[240] In other words, developers

---

234. *See supra* notes 61–66 and accompanying text.

235. Evans, *supra* note 106, at 4 ("Calling the container a coin causes confusion because, at least at the start of the platform, the container is not a currency, since it is not widely used, and because the public ledger platform could be viable even if the container did not evolve into being a general-purpose currency.").

236. SWANSON, *supra* note 37, at n.55.

237. *Id*.

238. *See, e.g.*, Jay Cassano, *What Are Smart Contracts? Cryptocurrency's Killer App*, FAST CO. LABS (Sept. 17, 2014), http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app [https://perma.cc/YU3Y-MLKP] (explaining how smart-contract projects such as Ethereum and Codius are aimed at decreasing the monitoring and enforcement costs inherent in contracting).

239. This is an economic majority of 51 percent. *See supra* note 105; *see also* SWANSON, *supra* note 37 at 18, 28 (explaining that Bitcoin Improvement Proposals require community consensus in order to be implemented).

240. *See* SWANSON, *supra* note 37, at 13 ("An altcoin means 'alternate coin' – which commonly means any cryptocoin or cryptoledger that is not Bitcoin.").

with a novel vision for the ideal blockchain parameters set their own rules at the outset, according to a desired set of economic properties.[241] Some examples are Litecoin, a platform similar to Bitcoin but with faster transaction confirmations, an ideal feature for high-volume merchants;[242] Viacoin, a "notary" platform that time-stamps, transfers, and verifies ownership of documents;[243] and Storjcoin, a platform much different from Bitcoin that allows for a decentralized cloud storage system.[244]

Despite the excitement of this unbounded innovation, a system of parallel blockchains is inefficient and undesirable. They also pose significant risks to the sustainability and goodwill of the blockchain experiment. Although a full discussion of these risks exceeds the scope of this Note, they generally fall into one or more of the following categories: problems of initial distribution and valuation, liquidity shortages, adverse network effects, market fluctuations, fragmentation, security breaches, pump-and-dump market games, and plain fraud.[245] The good news, however, is that a recent development has shown these "worlds" of alternative-utility blockchains can coexist without the exchange-rate risk and other factors that make the current altcoin system unworkable.[246]

In October 2014, a group of leading developers introduced the concept of "sidechains."[247] Unlike altcoins, which require users to leave the Bitcoin platform, exposing them to significant risks,[248] sidechains are blockchains that are interoperable with one another and, most importantly, interoperable with the Bitcoin blockchain.[249]

---

241. *Id*.

242. LITECOIN, http://www.litecoin.org [http://perma.cc/SVYS-9DEN].

243. VIACOIN, http://viacoin.org [http://perma.cc/AGT6-6EHP].

244. STORJ, http://www.storj.io [http://perma.cc/WD67-FV5L].

245. *See* BACK ET AL., *supra* note 33, at 5 (describing these as problems with bitcoin and other cryptocurrencies); *see also* William J. Luther, *Cryptocurrencies, Network Effects, and Switching Costs* (Kenyon Coll., Mercatus Center Working Paper No. 13-17) (July 17, 2013) (on file with the *Duke Law Journal*) (analyzing the adverse impact of network effects and switching costs with respect to blockchain-based currencies like bitcoin). Given the legitimate policy issues around such "vaporware"—technology that is promised, but never fully developed—future scholarship in this area might consider whether the federal securities laws provide an appropriate mechanism for investor protection, particularly when such technology is centrally administered.

246. *See generally* BACK ET AL., *supra* note 33 (suggesting "sidechains" as a tool for avoiding these problems).

247. *Id*. at 1.

248. *See supra* text accompanying note 245.

249. BACK ET AL., *supra* note 33, at 5, 8.

By integrating with Bitcoin's blockchain, sidechains provide the benefits of altcoins without the accompanying risks. Such purpose-specific scripting will encourage further innovation[250] by allowing for a network of "distributed trust systems."[251]

B. Decentralized Smart Contracts and the Shape of Transactions to Come

Sidechains and scripting are changing how people think about blockchain technology. One broad area of innovation around these features is decentralized smart contracts.[252] Smart contracts are "computer protocols that facilitate, verify, execute and enforce the terms of a commercial agreement."[253] This concept is not new and is not unique to the blockchain. One primitive example is digital rights management (DRM), a technology developed to fight copyright infringement.[254] DRM technology essentially embedded U.S. copyright law into digital files by limiting the user's ability to view, copy, play, print, or otherwise alter the works.[255] In other words, digital audio files encrypted with DRM technology were not subject to the double-spending problem because they contained a basic smart contract, one that referenced a centralized network, (that is, Apple's server programmed to enforce the iTunes Store Terms and Conditions).[256]

The blockchain enables decentralized smart contracts—in other words, smart contracts that leverage a secure public ledger as an enforcement mechanism.[257] In contrast to the iTunes example, these

---

250. *See id*. at 7 ("[B]ecause sidechains are still blockchains independent of Bitcoin, they are free to experiment with new transaction designs, trust models, economic models, asset issuance semantics, or cryptographic features.").

251. *Id*. at 7. One expansive way to conceptualize the blockchain innovation is through the concept of "trustlessness"—the property of enabling all parties to verify on their own that information is correct without relying on trusting external parties for correct operation. *Id*.

252. *See* SWANSON, *supra* note 37, at 15–16 (introducing the concept of smart contracts and discussing their potential usefulness).

253. *Id*. at 11.

254. ROSS ANDERSON, SECURITY ENGINEERING 679 (2d ed. 2008); *see also* Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49, 60 (2008) (explaining the evolution of DRM technology).

255. Armstrong, *supra* note 254, at 60.

256. In 2009, Apple changed its policy and no longer provides DRM-encrypted digital files in its iTunes store. *See* Ruth Suehle, *The DRM Graveyard: A Brief History of Digital Rights Management in Music*, OPENSOURCE.COM (Nov. 3, 2011), http://opensource.com/life/11/11/drm-graveyard-brief-history-digital-rights-management-music [http://perma.cc/F94Q-3JDK].

257. For an extended discussion on decentralized smart contracts, see SWANSON, *supra* note

contracts do not rely on a third-party institution or server for centralized recordkeeping and enforcement. Because blockchain transactions are programmable and self-enforcing, parties might use smart contracts to design contractual relationships that are automatically executed without the additional costs of monitoring or enforcement.

This fact is significant. Intermediaries typically establish trust and reduce risk between counterparties to a transaction.[258] But with decentralized smart contracts, parties may transact at arms length, with total strangers, without the worry of fraud, and without the cost of third-party enforcement (that is, recordkeeping costs, mediation costs, and other administrative and operational costs). In other words, decentralized smart contracts allow for new markets to develop: disintermediated contract markets in which parties do not have concern for counterparty risk.[259]

Consider a smart-contracts market for futures trading.[260] Smart contracts in this market would be simple for two reasons. First, futures agreements involve objectively verifiable conditions about the state of the world—for example, the price of crude oil at a given time on the New York Mercantile Exchange. And second, futures agreements are highly standardized to ensure that contracts can be easily traded and priced.[261] Such an agreement would be self-

37, at 15–30.

258. DOUGLAS NORTH, INSTITUTIONS, INSTITUTIONAL CHANGE AND ECONOMIC PERFORMANCE 6 (1990).

259. Counterparty risk is the risk arising from the possibility that the counterparty may default on amounts owed on a transaction. THE NEW PALGRAVE DICTIONARY OF MONEY & FINANCE 502 (John Eatwell, Murray Milgate & Peter Newman eds., 1992).

260. For an extended analysis of smart contract markets and futures trading, see generally Trevor I. Kiviat, "Smart" Contract Markets: Trading Derivatives on the Blockchain (Apr. 2015) (unpublished manuscript), https://www.academia.edu/10766594 [http://perma.cc/2K8A-4HAW].

261. CME GROUP, A TRADER'S GUIDE TO FUTURES 4 (2013), https://www.cmegroup.com/education/files/a-traders-guide-to-futures.pdf [http://perma.cc/7ASG-6G3T]; *see also* Stephen G. Cecchetti, Jacob Gyntelberg & Marc Hollanders, *Central Counterparties for Over-the-Counter Derivatives*, BIS Q. REV., Sept. 2009, at 45, 49 ("[D]erivatives contracts have in many cases become more standardised. For example, over the years, *interest rate swaps* and foreign exchange derivatives have become highly standardised through voluntary industry initiatives."). This model is based on a hypothetical developed by Professor Houman B. Shadab in his remarks to the CFTC's Global Markets Advisory Committee. Houman B. Shadab, Professor of Law, New York Law School, Regulating Bitcoin and Block Chain Derivatives: Written Statement to the Commodity Futures Trading Commission 15 (Oct. 9, 2014), http://www.cftc.gov/ucm/groups/public/@aboutcftc/documents/file/gmac_100914_bitcoin.pdf [http://perma.cc/XL9G-5WXU].

monitoring and self-enforcing through a combination of scripting,[262] multi-sig,[263] and oracles, systems set up to monitor off-blockchain information and data that is essential to the effective execution of the smart contract's terms.[264]

In sum, the technology's potential to lower transaction costs with respect to contracting and transferring title to physical and personal property should generate special interest in the legal community. To be sure, there are challenges. First, the task of encoding the legal subtleties and nuances that underlie even the most basic contract poses significant programming challenges. And second, it is not clear whether and how smart contracts fit within the legal frameworks of the Uniform Commercial Code and general common law. Although an extended discussion of these two issues is beyond the scope of this Note, their serious analysis would add much to this nascent field.

CONCLUSION

Blockchain technology is adaptable and policymakers must view it as such. Regulation designed to mitigate the risks of such a powerful technology should be encouraged. However, policymakers should exercise caution and precision in tailoring the scope of regulation. As illustrated above, blockchain technology has utility beyond transmitting value in the traditional money-transmitter sense. Regulation aimed at the blockchain's money-transfer and payment functionalities must not create an unintentional chilling effect on this second category of functionalities.

States should monitor New York's BitLicense experiment and consider the issues raised in this Note as they consider their own models.[265] .For example, the NYDFS has recognized that BitLicense is

---

262. *See supra* Part III.A.

263. *See supra* note 213 and accompanying text.

264. "Off-blockchain" events are any measurable events that occur outside of the blockchain and thus cannot be monitored by an on-blockchain script. The current temperature in Durham, North Carolina; the spot price of Brent crude at a particular time in the future; and the results of the 2015 NCAA Men's Basketball Tournament are all off-blockchain events that could be referenced in a smart contract and enforced by an oracle.

265. It is likely that many such codes will be based on the Conference of State Bank Supervisors Draft Model Regulatory Framework for Virtual Currency Activities. *See* CONF. STATE BANK SUPERVISORS, STATE REGULATORY REQUIREMENTS FOR VIRTUAL CURRENCY ACTIVITIES: CSBS MODEL REGULATORY FRAMEWORK (Sept. 15, 2015), https://www.csbs.org/regulatory/ep/Documents/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf [http://perma.cc/USP3-U5WX].

intended only to apply to financial intermediaries.[266] This Note highlighted some ambiguity around "nonfinancial" use language.[267] Further, depending on particular alternative applications of blockchain technology, some additional guidance and regulation may need to occur outside of the BSA and state banking frameworks. For example, smart contracts that enable equity crowdfunding[268] should fit squarely in the domain of federal securities law, triggering registration and disclosure requirements and subjecting participants to SEC enforcement rules. In other words, policymakers must carefully define the specific activities that they seek to regulate. A basic understanding of the concepts set forth in this Note would be a strong starting point. To borrow from technologist Mark Stefik's words on the Internet, blockchain technology can support different kinds of dreams: "We choose, wisely or not."[269]

266. DAVIS POLK & WARDWELL LLP, *supra* note 39.

267. *Id*.

268. *See* SWANSON, *supra* note 37, at 83 (describing "crowdequity" as a potential tool for incentivizing early adoption by giving an equity stake to early users).

269. Mark J. Stefik, *Epilogue: Choices and Dreams*, *in* INTERNET DREAMS: ARCHETYPES, MYTHS, AND METAPHORS 390 (Mark J. Stefik ed. 1996).

VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SUMMER 2015 UNIVERSITY OF VIRGINIA VOL. 19, NO. 03

The Case for the Regulation of Bitcoin Mining as a Security

BENJAMIN AKINS, JENNIFER L. CHAPMAN & JASON GORDON †

† Benjamin Akins, JD, LLM is an Assistant Professor of Legal Studies and Taxation at Georgia Gwinnett College in the School of Business. Jennifer L. Chapman, JD, CPA is a Senior Lecturer at the J.M. Tull School of Accounting in the Terry College of Business at the University of Georgia. She is the Director of the MAcc Program and the Tull School AACSB Coordinator. Jason Gordon, JD, LLM, MBA is an Assistant Professor of Legal Studies and Management at Georgia Gwinnett College in the School of Business.

ABSTRACT

Bitcoin is rapidly increasing in use throughout the world. The process for introducing new bitcoin into the system is known as "mining." Mining, which is instrumental to the bitcoin system, involves the use of powerful computer systems and complex, computational algorithms to verify or validate prior bitcoin transactions. The reward for successfully undertaking this process is the creation and award of new bitcoin to the miner. Bitcoin mining has become a tedious and difficult process. The race to verify transactions, and thereby earn bitcoin, necessitates more sophisticated processes for verification and greater computational power.

Many bitcoin miners band together in groups called "pools" to create a powerful mining platform. Some miners invest time and effort to build or maintain a suitable computer system, while others passively provide money or other resources toward the creation of the mining system. Many such mining pools have grown to allow individuals to collectively contribute effort to the transaction verification process in exchange for an interest in the proceeds from the mining activity. The bitcoin mining pool has largely escaped regulation. This paper argues that the mining pool should be regulated under the existing federal securities regulation regime.

TABLE OF CONTENTS

I. INTRODUCTION

Bitcoin is a form of digital currency, known as cryptocurrency,[1] that has steadily risen in popularity since its origin. The current market capitalization is nearly $3 billion worldwide.[2] The cryptocurrency's appeal lies, at least in part, in the anonymity of bitcoin users and the low transaction costs of dealing in bitcoin.[3] The bitcoin system depends upon a process known as mining, by which individuals or groups of individuals use sophisticated computer systems to validate bitcoin transactions.[4] Successfully completing the validation process results in an award to the anonymous miner of newly generated bitcoin.[5] Mining is the sole method of introducing new bitcoin into the bitcoin network.[6]

A popular practice among bitcoin miners is to organize into groups known as "mining pools" to collectively mine for

---

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 8 (2008) (unpublished white paper), *available at* http://bitcoin.org/bitcoin.pdf, 2 (stating that "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" when explaining the bitcoin system.).
[2] *See* http://coinmarketcap.com (last visited Jan. 19, 2015) (showing current cryptocurrency market capitalizations).
[3] Joshua J. Doguet, Comment: *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119, 1119 (2013).
[4] *Introduction,* BITCOIN WIKI, https://en.bitcoin.it/wiki/Introduction (lasted visited Jan. 23, 2015) (explaining the bitcoin mining process).
[5] *Id*.
[6] *FAQ*, BITCOIN WIKI, https://en.bitcoin.it/wiki/FAQ#How_are_new_bitcoins_created.3F (last visited Jan. 19, 2015) ("New bitcoins are generated by the network through the process of '*mining*.'").

bitcoin.[7] While some individuals actively take part in assembling resources and employing a computer system to mine bitcoin (i.e., computationally verify prior transactions), others invest funds or the work product from their individual mining efforts into the mining pool in hopes of gaining a profit from the collective mining efforts.[8] These mining pools and the activities of their participants are largely unregulated.[9]

In this article, we propose that bitcoin mining pools are properly subject to regulation under existing federal securities laws. In particular, the mining pools meet the definition of an investment contract, and the resulting business relationship should qualify the mining pool for regulation as a security. In Part II, we begin by reviewing the process for mining bitcoin and survey existing bitcoin mining pool arrangements. In Part III, we explain the existing regulatory framework for the offering or sale of securities, and evaluate whether the bitcoin mining pool relationship constitutes a "security" under existing securities laws. We conclude that applying existing securities regulations to bitcoin mining pools is proper in light of the

---

[7] *See Pooled Mining*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Pooled_mining (lasted visited Jan. 23, 2015) ("Pooled mining is a mining approach where multiple generating clients contribute to the generation of a block, and then split the block reward according [to] the contributed processing power.").

[8] *Id*.

[9] To date, the IRS has issued a Notice addressing the income tax treatment of bitcoin transactions, but no other explicit federal regulatory action has been adopted regarding the cryptocurrency. Notice 2014-21, 2014-16 I.R.B. 938–40. *See also* Benjamin Akins, Jennifer L. Chapman, & Jason M. Gordon, *A Whole New World: Income Tax Considerations of the Bitcoin Economy*, 12 PITT. TAX REV. (2015) (discussing need for federal regulatory guidance on income taxation of bitcoin and the unofficial guidance contained in Notice 2014-21).

economic realities of bitcoin mining pools and would serve the stated purpose of securities law in protecting consumers.

II. BITCOINS AND THE MINING PROCESS

A. What is Bitcoin and How Does the System Function?

As stated above, bitcoin is a form of digital currency created, managed, and traded within an intricate network of interconnected computers.[10] The members must connect their computers to the peer-to-peer network to be a part of the bitcoin system.[11] Industry developments have attempted to develop physical representations to facilitate the trading of bitcoin,[12] but the actual bitcoin exists only as a digital file within the bitcoin system.[13] Bitcoin is not maintained as individual units; rather, a single digital file may represent (or contain) any number of bitcoin.[14] Individuals trade in bitcoin directly with other members of the system by authorizing the

---

[10] Tom Simonite, *What Bitcoin Is, and Why It Matters*, MIT TECH. REV. (May 25, 2011), *available at* http://www.technologyreview.com/computing/37619 (providing an overview of the development of the bitcoin system); Omri Marian, *Are Cryptocurrencies Super Tax Havens?* 112 MICH. L. REV 38, 41. (2013) ("The most known, and currently the most successful example of cryptocurrency, is the Bitcoin, first introduced in 2008.").

[11] *See* Nakamoto, *supra* note 1, at 3.

[12] See, *e.g.*, *Physical Bitcoins by Casascius*, *available at* https://www.casascius.com (last visited Jan. 25, 2015), for an example of a company producing a physical bitcoin for exchange.

[13] *See* Nakamoto, *supra* note 1, at 2.

[14] *See* Bitcoin Developer Guide, BITCOIN, *available at* https://bitcoin.org/en/developer-guide#block-chain ("A single transaction can create multiple outputs, as would be the case when sending to multiple addresses, but each output of a particular transaction can only be used as an input once in the block chain.").

transfer of a bitcoin file, or some fraction thereof, to the other member's electronic wallet.[15] Bitcoin wallets, like physical wallets, house the digital bitcoin files.[16] The wallet can either be located in the cloud or on a member's computer hard drive.[17] While the transfer of bitcoin takes place from wallet to wallet,[18] the location of the wallet is identified by what is known as public and private keys.[19] The public key is similar to the address of the wallet and known by other members of the bitcoin system.[20] The private key is kept private and is used in conjunction with the public key to authorize or accept a transfer of bitcoin to the wallet.[21] The intended transaction,

---

[15] *See* Nakamoto, *supra* note 1, at 2 (explaining that members of the bitcoin system transfer the bitcoin through electronic transmission of information).

[16] *See* Some Bitcoin Words You Might Hear, *available at* http://bitcoin.org/en/vocabulary#bitcoin (lasted visited Jan. 23, 2015) ("A Bitcoin wallet is loosely the equivalent of a physical wallet on the Bitcoin network.").

[17] *See* J.P., Virtual Currency, THE ECONOMIST (Jun. 25, 2015), *available at* http://www.economist.com/blogs/babbage/2011/06/virtual-currency (noting the storage of bitcoin in digital wallets located on a computer hard drive and the use of online digital wallets).

[18] *See* Bitcoin Developer Guide, BITCOIN, *supra* note 14 ("Permitting receiving and spending of satoshis [an amount of bitcoin] is the only essential feature of wallet software…").

[19] *See* Some Bitcoin Words You Might Hear, *supra* note 16 ("Your private key(s) are stored in your computer if you use a software wallet; they are stored on some remote servers if you use a web wallet. Private keys must never be revealed as they allow you to spend bitcoins for their respective Bitcoin wallet.").

[20] Nikolei M. Kaplano, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 116 (2012) ("Essentially, the public key is like an email address—public and available to everyone—while the private key is like the password needed to authorize messages (in this case bitcoins) to go in and out.").

[21] *Id*.

absent identifying information, is broadcast to the bitcoin system for verification.[22]

Bitcoin files exist as a blockchain containing the history of all transactions of that particular bitcoin file.[23] With each transaction the blockchain grows and makes it increasingly difficult to trace the origins of the file.[24] Members of the bitcoin system (individually or collectively) work to identify and verify the veracity of exchanges of existing bitcoin between other members.[25] As previously discussed, this verification process is know as mining, and it is the sole manner by which new bitcoins enter the system.[26] Successful verification of the previous transaction creates new bitcoin in the system, which is then awarded and deposited into the designated wallet of the verifying member.[27] As such, the number of bitcoins in the system rises as the number of bitcoin transactions and successful verifications increase. In this manner, the specific value is derived from the amount of

---

[22] Nakamoto, *supra* note 1, at 3.

[23] *How Bitcoin Works*, BITCOIN WIKI, https://en.bitcoin.it/wiki/How_bitcoin_works (lasted visited Jan. 23, 2015) ("This complete record of transactions is kept in the block chain, which is a sequence of records called blocks.").

[24] Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 160, 167 (2011) ("the problem difficulty has increased so much that most computers would now take on average a year or more to mine just 50 BTC [now 25 BTC].").

[25] *See* Kaplano, *Nerdy Money, supra* note 20, at 119–21 (describing the mining process and the introduction of new bitcoin into the system).

[26] *See Introduction*, BITCOIN WIKI, *supra* note 4 (explaining the mining process).

[27] Grinberg, *supra* note 24, at 163 ("New bitcoins are issued to competing "miners" who use their computers to generate solutions to problems that help ensure the integrity and security of the system.").

demand for the bitcoin and the supply available in the bitcoin system.[28]

As stated above, bitcoin miners perform the dual role of verifying bitcoin transactions and, through their verification efforts, introducing new bitcoin into the system. The bitcoin system contains information about every bitcoin transaction that has ever taken place.[29] To successfully mine bitcoin, an individual must employ an algorithm to trace the transaction history of a given block chain.[30] Specifically, the miner must work backwards from the present transaction and piece together the prior transactions that make up the blockchain of the bitcoin involved in the present transaction.[31] The verification process is extremely onerous and is prohibitively slow and difficult to calculate without the assistance of computer processors.[32] Once the system verifies the transfer, the new transaction details become part of the bitcoin blockchain.[33] The member or members of the system to first

---

[28] *Frequently Asked Questions*, BITCOIN, http://bitcoin.org/about.html (lasted visited Jan. 23, 2015).

[29] Danielle Drainville, *An Analysis of the Bitcoin Electronic Cash System*, Uwaterloo.com 11 (2012), *available at* https://math.uwaterloo.ca/combinatorics-and-optimization/sites/ca.combinatorics-and-optimization/files/uploads/files/Drainville,%20Danielle.pdf (lasted visited Jan. 23, 2015) ("This is the first block in the chain and was generated on January 3, 2009 by Satoshi Nakamoto.").

[30] *How Does Bitcoin Work?*, http://bitcoin.org/en/how-it-works, (lasted visited Jan. 23, 2015) (describing the use of complex algorithms to verify bitcoin transactions).

[31] *See id.*, ("In order to preserve the integrity of the block chain, each block in the chain confirms the integrity of the previous one, all the way back to the first one, the genesis block.").

[32] Grinberg, *supra* note 24, at 167.

[33] Nakamoto, *supra* note 1, at 3.

accurately verify the transaction are awarded 25 bitcoin by the system.[34]

B. Bitcoin Mining Pools as Investment Activity

The difficulty and expense associated with mining bitcoin has given rise to groups or collectives, known as "mining pools," who work together to mine bitcoin.[35] Members of a mining pool perform small portions of the transaction verification process. They then provide these pieces of work to the mining pool operator, who assembles the pieces of work in an attempt at verifying a given blockchain.[36] Members of the mining pool receive a benefit for their contibution to the effort of verifying a transaction. The individual miner's compensation is based upon a percentage or share of the bitcoin mined in a given transaction or over a series of transactions.[37] The miner's share is in turn measured by her contribution (her "proof of work") that demonstrates a portion of a blockchain that the miner has successfully mapped.[38]

As discussed above, mining pools involve the investment of individual effort to be combined with the efforts of others to produce or generate bitcoin as a reward. As with any investment, the decision of whether to invest effort in a

---

[34] *See* generally, Bitcoin CZ Mining, http://mining.bitcoin.cz/ (explaining the manner in which bitcoin is awarded and divided after successful mining).

[35] *See Pooled Mining*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Pooled_mining (lasted visited Jan. 23, 2015) ("Pooled mining is a mining approach where multiple generating clients contribute to the generation of a block, and then split the block reward according [to] the contributed processing power.").

[36] *Id*.

[37] *Id*.

[38] *Id*.

mining pool turns upon the expected return for that effort. Each miner's expected return varies depending upon numerous factors, including the miner's individual share of the pool and the total value of the mined bitcoin.[39]

Existing bitcoin mining pools employ numerous methods of compensating the miners.[40] For example, an early method known as the "proportional approach" rewards individual miners based on the proportion of work provided once an entire blockchain is verified.[41] Another common method, known as "pay-per-share," compensates individual miners for a specific amount of work (proof of work completed) contributed to the pool.[42] This relationship ensures the individual miner of compensation, regardless of whether the collective mining effort produces bitcoin. The downside of this arrangement is that it requires a significant reserve of bitcoin to maintain sufficient liquidity to compensate the miners in the event a mining effort is fruitless.[43] Numerous other methods now exist in an effort to shift the risk and redistribute compensation rates among individual miners and the pool operator.[44] A miner's compensation will, therefore,

---

[39] *See Mining Pool Reward FAQ - Bitcoin*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Mining_pool_reward_FAQ (last visited Jan. 23, 2015) (explaining the method of allocating shares to contributors to a successful mining pool.)

[40] *See Bitcoin Mining Pools*, BITCOINMINING.COM, http://www.bitcoinmining.com/bitcoin-mining-pools/ (last visited Jan. 19, 2015) (explaining various pooled payment methods presently in use).

[41] *Id*.

[42] *Id*.

[43] *Id*.

[44] *Bitcoin Mining Pools*, BITCOINMINING.COM, *supra* note 40. Examples of compensation schemes include: Pay Per Last N Shares (PPLN), Double Geometric Method (DGM), Shared Maximum Pay Per Share (SMPPS), Equalized Shared Maximum Pay Per Share (ESMPPS), Recent Shared Maximum Pay Per Share (RSMPPS), Capped Pay Per Share with Recent

vary depending upon which scheme is used by a given mining pool.[45]

Despite the various compensation regimes, the core principle of the mining pool is that individuals produce work product that has a greater value when combined with the work product of others. Unlike in organizations where individuals work in concert, mining pools involve the assembly of independent work product created by potentially unknown or unrelated individuals. The fact that individual miners input or invest their work product into a mining pool with the purpose of receiving a share of the proceeds from the present or ongoing mining activity calls into question the applicability of security laws to the mining pool operations.

III. BITCOIN MINING POOLS AS SECURITIES

A. What is a Security?

1. The Statutory Definition of a Security

The answer to the question, "what constitutes the sale of securities?" is far less obvious than the phrase implies. The Securities Act of 1933 ("1933 Act") provides that "[t]he term 'sale' or 'sell' shall include every contract of sale or disposition of a security or interest in a security, for value."[46] The courts

---

Backpay uses a Maximum Pay Per Share (MPPS), Bitcoin Pooled mining (BPM), Pay on Target (POT), SCORE, ELIGIUS, and Triplemining methods. The exact contours of each approach are beyond the scope of this article.

[45] *Id*.

[46] Securities Act of 1933 § 2(a)(3); 15 U.S.C. § 77b(a)(3) (2014). The 1934 Securities Exchange Act § 3(a)(10), 15 U.S.C. § 78c(a)(10) (2014), which

have construed the term "sale" to include any transfer or subsequent retention of interest in a security as part of a transaction.[47] In contrast, the term "security" is defined in far broader terms. Section 2(a)(1) of the 1933 Act provides a very long list of what constitutes a security, determining whether an item is a security begins with a two-part approach.[48] First, any "note," "stock," "bond," or "debenture" is essentially a transferable share or interest in a business and is a security.[49] The second category includes "any evidence of indebtedness," "certificate of interest or participation in any profit-sharing agreement," "any investment contract," and any "instrument commonly known as a 'security.'"[50] Both definitions apply "unless context otherwise requires."[51]

These categories leave open for interpretation whether a type of interest or instrument is a security under each category. The courts, using standard principles of statutory construction, often begin their analysis by looking at Congress' intent.[52]

---

regulates the sale of such items on public exchanges, contains a definition nearly identical to the one under the 1933 Act.

[47] *See, e.g.*, Pinter v. Dahl, 486 U.S. 622, 643–44 (1988) (noting the Courts' broad interpretation of sales); Rubin v. United States, 449 U.S. 424, 430 (1981) ("It is not essential under the terms of the Act [section 2(3)] that full title pass to a transferee for the transaction to be an 'offer' or a 'sale.'"); SEC v. Datronics Engineers, Inc., 490 F.2d 250, 253–54 (4th Cir. 1973), *cert. denied*, 416 U.S. 937 (1974) (finding the disposition of new stock among existing shareholders constituted a sale).

[48] Securities Act of 1933 § 2(a)(1), 15 U.S.C. § 77b(a)(1) (2014).

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *See generally* Reves v. Ernst & Young, 494 U.S. 56, 60–62 (1990) (noting Congress' intent to regulate the market sufficiently broad to include nearly any security instrument); United Housing Foundation, Inc. v. Forman, 421 U.S. 837, 847–48 (1975) (noting that Congress intended the definition of securities to be broad and encompass numerous types of

Congress' purpose in enacting securities regulation was to prevent fraud on the public.[53] Succinctly stated, the history of the development of securites regulation began at the state level with so-called "blue sky laws" and were followed by a comprehensive federal scheme to add uniformity across states.[54] Within the categories of security described in the federal securities laws, courts have developed multiple tests to determine whether a particular type of investment constitutes a security.[55] Perhaps most notably, the investment contract category is essentially a "catch-all" provision whereby lots of unique instruments or interests constitute a security. It is this category which seems most applicable to bitcoin mining.

2. Development of a Common Law Approach

The first iteration of the modern test for determining what constitutes an investment contract was laid out in *SEC v.*

---

arrangements); SEC v. W.J. Howey Co., 328 U.S. 293, 298–99 (1946) (discussing the origin of the term "investment contract" as it relates to Congress' intention in regulating these arrangements); s*ee also* Kyle M. Globerman, *The Elusive and Changing Definition of a Security: One Test Fits All*, 51 FLA. L. REV. 271, 292 (1999) (noting that the broad definition of a security meets the intent of Congress in passing the securities acts as preventing fraud).

[53] Globerman, *supra* note 52, at 288 ("[T]he reach of the Securities and Exchange Acts should cover all transactions that attempt to defraud public investors.").

[54] *See generally* Darlene S. Wood, Case Note*: Lease-back Arrangements are Investment Contracts and Therefore Securities Under the Securities Acts: SEC v. Edwards*, 7 DUQ. B.L.J. 135, 140–44 (2005) (outlining the history and need behind the creation of the Securities Acts from state blue sky laws to the adoption of *Howey*).

[55] Seed McGinty, *What is a Security*, 1993 WIS. L. REV. 1033, 1036 (1993) (supporting the common law history of multiple tests for determining whether an instrument is an investment contract and, therefore, a security).

W.J. Howey Co.[56] In this case, Howey sold parcels of citrus groves to investors.[57] Investors took no part in cultivation of the groves, but entered into an attached 10-year service contract with Howey for cultivation.[58] Howey would harvest the oranges from all of the groves and then pay investors a percentage of the total yield based upon the number of parcels owned.[59] The Securities and Exchange Commission (SEC) challenged this practice, indicating that the arrangement constituted the sale of "investment contracts" to which the registration requirements apply.[60] The Supreme Court agreed with the SEC that the investors' interests in the citrus groves were securities and, for the first time, explicitly ennumerated the elements of an "investment contract" as: 1) an investment of money, 2) into a common enterprise, 3) with the expectation of profits, and 4) derived solely from the efforts of others (the "*Howey* Test").[61] In applying the above elements of an investment contract, the *Howey* Court examined the economic reality of the situation.[62] That is, the Court adopted an approach that reviews function over form. In doing so, the court expressly recognized that the 1933 Act's "investment contract" provisions should be construed broadly to cover "a variety of situations where individuals were led to invest money in a common enterprise with the expectation that they would earn a profit solely from the efforts of the promoter or of someone other than themselves."[63]

---

[56] SEC v. W. J. Howey Co., 328 U.S. 293 (1946).
[57] *Id*. at 294–95.
[58] *Id*. at 295–96.
[59] *Id*.
[60] *Id*. at 297–98.
[61] *Id*. at 300–01.
[62] *Id*. at 298.
[63] *Id*.

Following the *Howey* decision, in *United Housing Foundation, Inv. v. Forman*, the Supreme Court employed the *Howey* Test to determine if a cooperative housing corporation that required its residents to buy "shares" of the co-op constituted a security.[64] Money from the sale of these shares was used to defray initial costs of establishing and managing the cooperative.[65] After the costs of these shares generally rose as the rent costs in the cooperative went up, the tenants/shareholders sued saying they were deceived in the purchase of these securities, as they were not informed that the stock's price would rise.[66] As in *Howey*, the Court emphasized the "economic realities" of the transaction.[67] The cooperative's use of the word "stock" to refer to the fees associated with membership in the cooperative was not determinative of whether such payments or fees constitute a security.[68] In examining the economic reality of the transaction, the Court found no typical indicia of a security.[69] Applying the *Howey* Test, the Court determined the purported "stock" was not purchased in expectation of profits, but rather "solely by the prospect of acquiring a place to live."[70] The effect of this decision was to reinforce the use of the economic realities of the situation when applying the *Howey* Test to a purported investment contract.

---

[64] United Housing Foundation, Inc. v. Forman, 421 U.S. 837, 840 (1975).
[65] *Id*. at 841.
[66] *Id*. at 844–45.
[67] *Id*. at 850–52.
[68] *Id*. at 848.
[69] *Id*. at 851.
[70] *Id*. at 853.

3. Refining What Constitutes an Investment Contract

Building upon the precedent established in *Howey*, courts have continued to apply and modify specific elements of the *Howey* Test in determining whether a transaction constitutes the sale of a security. These refinements shed further light not only on the breadth of the investment contract category of securities but also on the extent to which the determination that a given transaction falls within this category depends upon the economic reality of that transaction. Thus, a review of the status of each element of the *Howey* Test proves helpful.

a. Investment of Money

The initial *Howey* Test element requires an investment of money.[71] For example, in *Uselton v. Commercial Lovelace Motor Freight, Inc.*, four hundred former employees of a motor freight company sued alleging, *inter alia*, violations of the federal securities laws.[72] Following the sale of the company to the defendant, the company invited the employees to participate in a wage reduction program in return for an interest in a stock ownership plan and a profit sharing plan.[73] The district court found that the scheme violated the first prong of the *Howey* Test, as no investment of money occurred.[74] The Tenth Circuit disagreed, stating, "it is well established that cash is not the only form of contribution or investment that will create an investment contract. Instead, the 'investment' may

---

[71] *W.J. Howey Co.*, 328 U.S. at 301.
[72] Useton v. Commercial Lovelace Motor Freight, Inc., 940 F.2d 564, 570 (10th Cir. 1991).
[73] *Id*.
[74] *Id*. at 573.

take the form of 'goods and services' or 'some other exchange of value.'"[75] The court went on to clarify the proper legal standard—whether the economic realities demonstrated that the plaintiff made an investment in the transaction or that the transaction as a whole involved "an exchange of value."[76]

In contrast, in *International Brotherhood of Teamsters v. Daniel*,[77] the Supreme Court held that investments made by the manager of an employee's compulsory pension plan did not constitute an investment contract.[78] The employees did not make contributions to the plan; rather, they vested in benefits through years of service. The contribution of work to the company by the employees, as opposed to direct funds into the pension plan, resulted in the arrangement failing the *Howey* Test.[79] In other words, unlike the arrangement in *Uselton*, the economic reality of a transaction whereby a company invests money in a retirement plan on behalf of an employee fails to equate to an investment of money by the employee. As such, the transaction failed the first prong of the *Howey* Test.[80]

---

[75] *Id*. at 574 (internal citations omitted).
[76] *Id*. at 575; *see also* Dubin v. E.F. Hutton Group, Inc., 695 F. Supp. 138, 145–46 (S.D.N.Y. 1988) (finding the formation of an equity ownership plan as part of an employment agreement is a security); Yoder v. Orthomolecular Nutrition Inst., Inc., 751 F.2d 555, 560–61 (2d Cir. 1985) (supporting the proposition that equity ownership as part of employment constitutes "investment of money" under the *Howey* Test).
[77] 439 U.S. 551 (1979).
[78] *Id*. at 560–61.
[79] *Id*.
[80] *Id*.

b. Common Enterprise

The "common enterprise" element[81] of the *Howey* Test continues to be the subject of extensive common law interpretation. Courts applying the *Howey* Test have generally adopted one of three main approaches to this element: horizontal commonality, strict vertical commonality, and broad vertical commonality.[82]

Horizontal commonality requires that contributions of funds from investors be pooled together as a common investment.[83] While this test requires that an investment contract involve more than a single investor,[84] it is possible that multiple investors can constitute a single investment unit that fails the multiple investor requirement. For example, in *Milnarik v. M-S Commodities, Inc.*,[85] a small group invested funds in a commodity trading account controlled by a money manager.[86] The Seventh Circuit held that there was no unified investment decision by the investors, and the use of an investment manager as a common agent to manage funds did not establish an investment contract.[87] The court reinforced this strict pooling requirement in subsequent cases.[88] The horizontal

---

[81] SEC v. W.J. Howey Co., 328 U.S. 293, 298–99 (1946).
[82] *See generally* Maura K. Monaghan, Note, *Financial Services Regulation: A Mid-Decade Review: An Uncommon State of Confusion: The Enterprise Element of Investment Contract Analysis*, 63 FORDHAM L. REV. 2135 (1995) (discussing the various judicial applications of the *Howey* "common enterprise" element).
[83] Steinhardt Group, Inc. v. Citicorp, 126 F.3d 144, 151 (3d Cir. 1997).
[84] Curran v. Merrill Lynch, Peirce, Fenner & Smith, Inc., 622 F.2d 216, 222–23 (6th Cir. 1980).
[85] 457 F.2d 274 (7th Cir.), *cert. denied*, 409 U.S. 887 (1972).
[86] *Milnarik*, 457 F.2d at 275.
[87] *Id.* at 275–79.
[88] Hirk v. Agri-Research Council, Inc., 561 F.2d 96 (7th Cir. 1977).

commonality element also requires that investors have a common interest in the success of the venture.[89] This provision has been interpreted to mean that any profits or losses derived from the common investment must be distributed to investors pro-rata based upon their contributions.[90]

Strict vertical commonality looks beyond the common situation of investors and requires that the investor and investment manager or promoter have similar economic interests.[91] That is, the investment manager's success must depend upon the success of the investor. As such, the type of risk shared in the venture is the same.[92] Strict vertical commonalty first appeared in the Ninth Circuit's analysis in *SEC v. Glenn W. Turner Enterprises.*[93] The court stated that, "[a] common enterprise is one in which the fortunes of the investor are interwoven with and dependent upon the efforts and success of those seeking the investment or third parties."[94] The strict vertical commonality approach was later applied in *SEC v. R.G. Reynolds Enterprises, Inc.*[95] The court paid little regard to the pooling of funds or the investor's reliance on the investment manager's skill; rather, it focused upon the sharing

---

[89] *Curran*, 622 F.2d at 224.
[90] *Id*. at 222–23.
[91] *See* Mordaunt v. Incomco, 686 F.2d 815, 817 (9th Cir. 1982), *cert. denied*, 469 U.S. 1115 (1985).
[92] *See* Brodt v. Bache & Co., Inc., 595 F.2d 459, 462 (9th Cir. 1978) ("Appellant's enterprise was a "solitary" one. His profits were shared neither with other investors nor the appellee; whether his investment flourished or perished was unrelated directly to either the general financial health of the appellee or the ability of the appellee to perform a duty, the purpose of which would be "to secure" to some extent the appellant's investment.").
[93] 474 F.2d 476, 482 (9th Cir.), *cert. denied*, 414 U.S. 82 (1973).
[94] *Id*. at 482 n7.
[95] 952 F.2d 1125 (9th Cir. 1991).

of risk. [96] The court held that allocating a management fee for the account manager resulted in a sufficient alignment of risk between investor and manager.[97] The key to this relationship was that the management fee was not a secured percentage of assets held; rather, it was based somewhat on the performance of those assets.[98]

The broad approach to vertical commonality focuses on the investor's dependence on the promoter,[99] rather than the nature of the risk shared by the parties.[100] More specifically, the courts applying this approach require that the investor depend heavily upon the level of skill or knowledge of the investor and her dependence upon the promoter in making the investment.[101] The broad-based approach to vertical commonality first appeared in *SEC v. Koscot Interplanetary, Inc.*[102] In *Koscot*, promoters sold shares in a pyramid type promotion, where managers would control and maintain the enterprise, while investors would be rewarded based on their ability to convince others to attend high-pressure sales meetings run by the promoters.[103] The court held that "the requisite commonality is evidenced by the fact that the fortunes of all investors are inextricably tied to the efficacy of the

---

[96] *Id*. at 1129.
[97] *Id*. at 1130–31.
[98] *See e.g*., Meyer v. Thomas & McKinnon Auchincloss Kohlmeyer, Inc. 686 F.2d 818 (9th Cir. 1982) (holding that an arrangement where a promoter is compensated with a percentage of the assets under his management does not amount to an investment contract).
[99] *See e.g*., SEC v. Koscot Interplanetary, Inc., 497 F.2d 473, 478 (5th Cir. 1974).
[100] Brodt v. Bache & Co., Inc., 595 F.2d 459, 461 (9th Cir. 1979); SEC v. Continental Commodities Corp, 497 F.2d 516, 522 (5th Cir. 1974).
[101] *Id*.
[102] 497 F.2d 473 (5th Cir. 1974).
[103] *Id*. at 475–76.

[promoters'] meetings."[104] The broad vertical commonality approach, therefore, centers upon the investor's reliance upon the promoter's skill in the area of investment.[105]

c. Expectation of Profit Derived Solely from the Efforts of Others

Following the passage of the Securities Act of 1933, the definition of investment contract has been subject to debate among the court.[106] The Supreme Court clarified the "expectation of profits" language from the first element of the *Howey* Test in *United Housing Foundation, Inc. v. Forman.*[107] In *Forman*, the Court said that the primary motivation for investing must be to achieve a return on the value invested.[108] Conversely, if investors are primarily driven by a motive other than profits—as they were in *Forman*—then the endeavor will fail this element of the *Howey* Test.[109]

The court in *SEC v. Glenn W. Turner Enterprises* addressed the next part of the *Howey* Test, "derived solely from the efforts of others," by focusing on the balance of effort between the investors and promoters.[110] Notably, the court held that the "solely" language in the *Howey* Test should not be

---

[104] *Id*. at 479.
[105] *See, e.g*., SEC v. Continental Commodities Corp, 497 F.2d 516, 522 (5th Cir. 1974) ("[T]he critical inquiry is confined to whether the fortuity of the investments collectively is essentially dependent upon promoter expertise.").
[106] William H. Newton, III, *What Is A Security: A Critical Analysis*. 48 MISS. L.J. 167, 167 (1977).
[107] 421 U.S. 837 (1975).
[108] *Id*. at 856–57.
[109] *Id*. at 851 ("In short, the inducement to purchase was solely to acquire subsidized low-cost living space; it was not to invest for profit.").
[110] 474 F.2d 476 (9th Cir. 1973), *cert. denied*, 414 U.S. 821 (1973).

strictly construed.[111] If it is, the court reasoned, the purpose of the securities regime would be defeated.[112] The court chose to focus on "whether the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise."[113]

Later, the Supreme Court in *SEC v. Edwards* applied *Howey* and reiterated that its standard was a flexible, not static, principle, under which Congress sought to "regulate investments, in whatever form they are made and by whatever name they are called."[114] The court found no reason to distinguish fixed from variable returns under *Howey* and saw no conflict with *United Housing* or any other precedent.[115] Specifically, the Court interpreted *United Housing*'s statements that profits meant either capital appreciation or participation in earnings as merely examples or passing dictum rather than

---

[111] *Id*. at 482.
[112] *Id*. ("Adherence to such an interpretation could result in a mechanical, unduly restrictive view of what is and what is not an investment contract. It would be easy to evade by adding a requirement that the buyer contribute a modicum of effort. . . . To do so would not serve the purpose of the legislation.").
[113] *Id*. *See also* Hocking v. Dubois, 885 F.2d 1449, 1455 (9th Cir. 1989) (holding that the focus should be on whose efforts are "significant" and "essential" in affecting the success of the endeavor).
[114] 540 U.S. 389, 391 (2004) (quoting Reves v. Ernst & Young, 494 U.S. 56, 61 (1990)). Within the text, the authors have used *Edwards* to refer to the line of cases which came to the Supreme Court on appeal from the Eleventh Circuit. At the Court of Appeals level, the case was originally cited as *SEC v. ETS Payphones, Inc*. SEC v. ETS Payphones, Inc. 408 F.3d 727 (11th Cir. 2005) (*on remand*); SEC v. ETS Payphones, Inc., 300 F.3d 1281 (11th Cir. 2002).
[115] *Id*. at 395.

constituting the only definition of profits.[116] Consequently, the Court reaffirmed its elemental test adopted in *Howey* as the appropriate standard under which to examine an investment contract and held that "an investment scheme promising a fixed rate of return can be an 'investment contract' and thus a 'security' subject to the federal securities laws."[117]

The Court remanded the *Edwards* case to the Eleventh Circuit,[118] which, in turn, addressed the issue of vertical and horizontal commonality.[119] The court in *Edwards* stated that "[b]road vertical commonality . . . only requires a movant to show that the investors are dependent upon the expertise or efforts of the investment promoter for their returns."[120] In a concurring opinion, Judge Lay went further, writing that vertical commonality amounted to nothing more than *Howey*'s third element—an expectation of profits to be derived solely from the efforts of others—and thus made *Howey* intrinsically

---

[116] *Id*. at 395–96 (noting that in *United Housing*, the Court "laid out two *examples* of investor interests that [it] had
found to be 'profits' and that the Court will not be bound "unnecessarily to passing dictum that would frustrate
Congress' intent to regulate [investment schemes].") (*emphasis added*) (*quotations in original*).
[117] *Id*. at 397 (*quotations in original*).
[118] United States v. Edwards, 540 U.S. 389 (2004), *rev'd and rem'd*, 526 F.3d 747 (11th Cir. 2008).
[119] 300 F.3d at 1285 (Lay, J., concurring).
[120] *Id*. at 1284. *See also* Curran v. Merrill Lynch, Peirce, Fenner & Smith, Inc., 622 F.2d 216 (6th Cir. 1980) ("[T]he
finding of a vertical common enterprise based solely on the relationship between promoter and investor is
inconsistent with *Howey*."); Milnark v. M-S Commodities, Inc., 457 F.2d 274, 275–77 (7th Cir. 1972);
Berman v. Bache, Halsey, Stuart, Shields, Inc., 467 F. Supp. 311, 319 (S.D. Ohio 1979).

redundant and its third element superfluous.[121] Indeed, the SEC conceded that broad vertical commonality was an inappropriate test for the same reason—it collapses the second and third elements.[122] Horizontal commonality, which requires a pooling of funds under which "individual investors share all the risks and benefits of the business enterprise," is thus the appropriate standard to examine the common enterprise element of *Howey*.[123]

B. Entity Relationships and the Sale of Securities

The definition of a security and the elements of an investment contract established in the *Howey* Test begs the question, what transactions concerning buisness entity relationships constitute the sale of a security interest? While the sale of an interest in a business entity to a third-party investor generally constitutes the sale of a security,[124] the formation of a new business entity by its founders is generally exempt from securities regulation under state and federal law.[125]

The formation of certain business relationships do not require the formal filing of a state-recognized business entity. For instance, a default partnership entity results from the collective effort of more than one individual with the intention

---

[121] 300 F.3d 1281, 1285 (Lay, J., concurring).
[122] *Id*. at 1286 (citing Brief for Appellant, SEC at 28 n.11, SEC v. SG Ltd., 265 F.3d 42 (1st Cir. 2001)).
[123] *Id*. at 1283–84.
[124] Securities Act of 1933 § 2(a)(1), 15 U.S.C. § 77b(a)(1) (2014) (An security includes any "stock" or ""certificate of interest or participation in any profit-sharing agreement").
[125] *Id*. at § 77d(a)(2) ("The provisions of section 77e of this title shall not apply to… (2) transactions by an issuer not involving any public offering.").

of sharing in any profits derived from the activity.[126] The formation of general partnerships has generally been held to not constitute the sale of a security.[127] In a general partnership, all of the partners have the right to be co-contributors and to share in any potential losses or liabilities of the business operations.[128] Several circuits, however, follow the approach established in *Williamson v. Tucker* when evaluating general partnership ownership interests for purposes of the securities laws.[129]

In *Williamson*, the Fifth Circuit provided a bright-line rule: a general partnership or joint venture can fall under the

---

[126] UNIF. P'SHIP ACT of 1997 § 202, Cmt. 1. [hereinafter "UPA"]. ("[A] partnership is created by the association of persons whose intent is to carry on as co-owners a business for profit, regardless of their subjective intention to be "partners." Indeed, they may inadvertently create a partnership despite their expressed subjective intention not to do so.").

[127] *See* Williamson v. Tucker, 645 F.2d 404, 421 (5th Cir. 1981), *cert. denied*, 454 U.S. 897 (1981) ("a general partnership or joint venture interest generally cannot be an investment contract under the federal securities acts"); *see also* Youmans v. Simon, 791 F.2d 341, 346 (5th Cir. 1976) ("federal securities laws are usually held not generally to apply to general partners." (citing Odom v. Slavik, 703 F.2d 212, 215 (6th Cir. 1983); Frazier v. Manson, 651 F.2d 1078, 1080 (5th Cir. 1981)); Douglas M. Fried, Note, *General Partnership Interests as Securities Under The Federal Securities Laws: Substance Over Form*, 54 FORDHAM L. REV. 303 (1985) (discussing how courts view general partnership interest under the securities framework in the wake of *Williamson*).

[128] *Williamson*, 645 F.2d at 421 (A general partner has a "legal right to a voice in partnership matters . . . " (quoting New York Stock Exchange, Inc. v. Sloan, 394 F. Supp. 1303, 1314 (S.D.N.Y. 1975)); *see also Youmans*, 791 F.2d at 346 ("The reason general partners are usually held not covered . . . is that they are entrepreneurs, not investors, and have the ability to take care of their own interests because of the inherent powers available to them. General partners may act on behalf of the partnership . . . and they are personally liable for all liabilities of the partnership.").

[129] *Williamson*, 645 F.2d at 421.

federal securities regime if plaintiffs can establish one of three elements.[130] First, the agreement must leave "so little power in the hands of the partner or venturer that the arrangement distributes powers as a limited partnership."[131] Alternatively, the partner must be so "inexperienced and unknowledgeable" that he is not intellectually able to assert the powers given to him in the agreement.[132] Finally, the endeavor will be treated as a security if the partner "is so dependent on some unique entrepreneurial or managerial ability" of the promoter that it would be impossible to replace them.[133]

Limited partnerships, in contrast, are unique in that only the general partner is personally responsible for losses or other liabilities of the venture.[134] As such, limited partnership interests may generally be considered securities.[135] In *Steinhardt Group, Inc. v. Citicorp*, however, the Third Circuit cautioned that the *Howey* Test must still be applied to limited partnership interests to determine if the limited partner is truly a passive investor.[136] The court concluded that, where limited partners can exert managerial efforts and hold certain voting

---

[130] *Id*. at 424.
[131] *Id*.
[132] *Id*.
[133] *Id*.
[134] *See Youmans*, 791 F.2d at 346 ("Limited partners, on the other hand, do not share the kind of authority wielded by general partners. Their liability for the partnership is limited to the amount of their investment.").
[135] *See id*. ("Limited partnership interests may be considered a security within the statutory definition" (citing Siebel v. Scott, 725 F.2d 995, 998 (5th Cir. 1984), 467 U.S. 1242 (1984))).
[136] 126 F.3d 144, 150 (3rd Cir. 1997) In *Steinhardt*, the plaintiffs believed they had been defrauded after they had purchased securitized pools of delinquent mortgage loans and properties belonging to defendant, Citicorp. *Id*. at 145. Finding that the first two prongs of the *Howey* Test had been met, the crux of the court's analysis focused on the third prong. *Id*. at 151-52.

powers, the third-prong of the *Howey* Test is not met and no investment contract exists.[137]

In summary, the determination of whether a business entity status constitutes a security rests with the level of control the investor has over the enterprise and the dependence of the investor upon the expertise or effort of the organizer or promoter. This analysis relates closely with the "solely from the efforts of others" element of the *Howey* Test. It provides a separate level of analysis of the relationship between parties to the activity to determine if that activity is subject to regulation as a security.

C. Mining Pools as Securities

The *Howey* Test, as refined by later court decisions, has been applied to a wide variety of property and transactions. By categorizing bitcoin mining as a security for purposes of the federal securities law, the United States could introduce a layer of regulation, without the need for novel or specialized laws, to address the new realities of the growing bitcoin economy. As described in the paragraphs that follow, the test can and should be applied to the bitcoin mining process. The structure of bitcoin mining pools fits comfortably within the four corners of the definition of "investment contract" as defined by *Howey* and its progeny—(1) an investment of money in a (2) common enterprise with (3) the expectation of profits (4) derived solely from the efforts of others.[138]

---

[137] *Id*. at 155.
[138] SEC v. W. J. Howey Co., 328 U.S. 293 (1946).

1. An Investment of Money

The first issue focuses on whether a share or interest in a mining pool constitutes an investment of money for the purposes of the first element of the *Howey* Test. To the extent individuals may purely invest money in a mining pool, this element is easily met. However, this requirement should not be read in an overly narrow manner so as to limit it only to an investment of legal tender. Some courts have interpreted the requirement of an investment of money broadly, focusing on the economic realities of the situation.[139]

In the context of mining pools, the value transferred to the pool is an element of completed work. The work, on its own, has little value; however, the investment has value when combined with the work product of others. Whether this transfer is deemed a transfer of services or as an "exchange of value," the investor would have made an investment under the *Howey* line of cases. Simply put, the economic realities of bitcoin mining are that all participants have invested in some way in the outcome of the mining—be it through a direct investment of money, the provision of goods or services to a bitcoin mining enterprise or a bitcoin mining pool, or through other exchanges of value. As such, the first element of the *Howey* Test is appears to be met for purposes of participants in a bitcoin mining pool.

2. Common Enterprise

As previously discussed, some courts break down the determination of whether a common enterprise exists into a determination of vertical and horizontal commonality.[140] In the

---

[139] *See supra* text accompanying notes 62–63.
[140] *See supra* text accompanying notes 82–105.

context of mining pools, horizontal commonality is easily established. The members meet the requirement that each individual investor share all the risks and benefits of the enterprise such that "fortunes of individual investors are inextricably intertwined by contractual and financial arrangements to that of any other investors."[141] The relationship among common stockholders in a corporation provides a prime example of the requirements of horizontal commonality. A common shareholder is a member of a common enterprise in which the profits are derived predominantly from the efforts of others, every investor has similar rights, preferences, and privileges, and, in their role as owners, shareholders play no part in the production of profits. Compared with the role of participants in a bitcoin mining pool arrangement, both groups collectively share profits and losses together, do not play an active part in the actual mining process, and, to the extent they receive a profit, those profits are based upon the successful efforts of those individuals actively involved in mining the bitcoin.

Vertical commonality requires "that the investors are dependent upon the expertise or efforts of the investment promoter for their returns."[142] Consistent with the explanation of broad vertical commonality in *Edwards,* the mining pool arrangement makes individual miners dependent upon the expertise and efforts of the mining pool operator in employing the contributed work.[143] Specifically, the promoter of the

---

[141] Cooper v. King, 1997 WL 243424 at *2 (6th Cir. 1997).
[142] SEC v. ETS Payphones, Inc., 300 F.3d 1281, 1284 (11th Cir. 2005) (*per curium*), *rev'd and rem'd sub nom*., SEC v. Edwards, 540 U.S. 389 (2004).
[143] *Id*.; s*ee also* Curran v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 622 F.2d 216, 224 (6th Cir. 1980) ("[T]he
finding of a vertical common enterprise based solely on the relationship between promoter and investor is

mining pool is tasked with assembling the work product of individual miners and employing that product in the transaction verification process.

When considering the broad and strict approaches to vertical commonality, it is important to note that the Fifth Circuit in *Edwards* simplified the original *Howey* analysis by providing that vertical commonality amounts to nothing more than *Howey*'s third element—an expectation of profits to be derived solely from the efforts of others—thus making the third element of the *Howey* Test superfluous.[144] Horizontal commonality, which requires a pooling of funds under which "individual investors share all the risks and benefits of the business enterprise," is thus the appropriate standard to examine the common enterprise element of *Howey*.[145]

Investors in a bitcoin mining pool, regardless of whether they actively participate in the mining process, share both the potential profits and losses from the pool. In essence, by spreading the costs and efforts among those involved in the pool, the pool's participants are able to make bitcoin mining economically more efficient. In return, they agree to share in the results of their collective efforts. As outlined above,[146] the various mining pools use a variety of approaches to divide their profits among the participants in the pool. Regardless of the

---

inconsistent with *Howey*."), *aff'd sub nom*. Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Curran, 456 U.S. 353 (1982); Milnarik v. M-S Commodities, Inc., 457 F.2d 274, 275–77 (7th Cir. 1972);
Berman v. Bache, Halsey, Stuart, Shields, Inc., 467 F. Supp. 311, 319 (S.D. Ohio 1979).

[144] *ETS Payphones*, 300 F.3d at 1285 (Lay, J., concurring).

[145] *Id*. at 1283–84.

[146] *See Bitcoin Mining Pools*, BITCOINMINING.COM, http://www.bitcoinmining.com/bitcoin-mining-pools/ (last visited Jan. 19, 2015) (explaining various pooled payment methods presently in use).

allocation method chosen, the core principle underlying a bitcoin mining pool is that a participant's individual efforts produce greater value when combined with the work product of other miners in the same pool. Such an arrangement reflects the very essence of a common enterprise.

3. Expectation of Profits Derived Predominantly From the Efforts of Others

In addition to a common enterprise, the *Howey* Test requires an expectation of profits from the investment. As previously discussed, bitcoin mining pools offer various methods of compensating the individual miner. Some of these methods involve fixed compensation to miners for work contributed. Other schemes make the receipt of profits contingent upon the success of the mining pool. Profits, for purposes of the *Howey* Test, may come in the form of fixed returns or contingent benefits. Per the Supreme Court's reasoning in *Edwards*, there is "no reason to distinguish between promises of fixed returns and promises of variable returns" when employing the *Howey* Test, as both produce a form of investment return.[147] The primary objective of Congress is not to separate methods of return; rather, it is to protect all investors in schemes dependent upon the efforts of others.[148] This element is meant to distinguish situations where the investor's motivation in making the purchase is to use or consume the item from situations where there is an expectation

---

[147] *Edwards*, 540 U.S. 389, 394 (2004).
[148] *Id*. at 394–95.

of profits[149] and requires that profits be derived "predominantly from the efforts of others."[150]

Thus, under *Howey*, if an investor controls the profitability of an investment, that investment is not a security.[151] As previously mentioned, the derived-from-the-efforts-of-others element generally requires an examination into the level of control retained by the investor. In the context of bitcoin mining, the individual miner loses all control of the process upon submitting his work product to the pool operator. "If the investor retains the ability to control the profitability of his investment, the agreement is not a security"[152] because the spirit of a security for investment purposes is the separation of influence between promoter and investor.[153] Typically, "[t]he investors provide the capital and share in the earnings and profits; the promoters manage, control, and operate the

---

[149] United Housing Foundation, Inc. v. Forman, 421 U.S. 837, 852–53 (1975).

[150]As originally worded, the *Howey* Test required that profits be derived solely from the efforts of others. *See* SEC v. Glenn W. Turner Enterprises, 474 F.2d 476, 482 (9th Cir.), *cert. denied*, 414 U.S. 821 (1973) ("Strict interpretation of the requirement that profits to be earned must come "solely" from the efforts of others has been subject to criticism. . . Adherence to such an interpretation could result in a mechanical, unduly restrictive view of what is and what is not an investment contract." (internal citations and footnotes omitted)).

[151] Albanese v. Florida Nat'l Bank of Orlando, 823 F.2d 408, 410 (11th Cir. 1987).

[152] SEC v. ETS Payphones, 300 F.3d 1281, 1285 (11th Cir. 2005) (*per curium*), *rev'd and remanded on other grounds sub nom.*, SEC v. Edwards, 540 U.S. 389 (2004) (quoting Albanese v. Florida Nat'l Bank of Orlando, 823 F.2d 408, 410 (11th Cir. 1987).

[153] *See* SEC v. Koscot Interplanetary, Inc., 497 F.2d 473, 478 (5th Cir. 1974) ("[T] he proper standard . . . is 'whether the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise.'" (quoting *Glen W. Turner Enterprises, Inc.*, 474 F.2d at 482)).

enterprise."[154] The Fifth Circuit in *Edwards* reasoned that by bargaining for a fixed return, investors may not have relied solely on the efforts of others because their contractually guaranteed returns "were derived as a benefit of [their] bargain under the contract."[155]

A primary draw of a bitcoin mining pool is that the arrangement allows persons who would not otherwise be able to mine bitcoin in an economically efficient manner to participate in the bitcoin economy. The individual participants may invest services and, in some cases other goods or resources, into the mining pool, while other participants in the same mining pool make similar or complimentary investments. Those investments combine to produce work product that ultimately produces value to be distributed among the members of the pool. However, for most participants in a mining pool, the return they receive from the mining pool, while dependent on their investment, is unrelated to their individual efforts. Rather, the efforts of the promoter in combining the work product of various pool participants into a useable fashion drives the generation of profits. In other words, for the vast majority of investors in a given bitcoin mining pool, any profit received is derived predominantly from the efforts of others. Thus, the final element of the *Howey* Test is met.

---

[154] SEC v. W.J. Howey, 328 U.S. 293, 300 (1946) (concluding that "arrangements whereby the investors' interests are made manifest involve investment contracts, regardless of the legal terminology in which such contracts are clothed.").
[155] *ETS Payphones*, 300 F.3d at 1285.

4. Bitcoin Mining Pools as a Business Entity or Organization

As previously discussed, forming either a general or limited partnership may constitute the sale or exchange of a security.[156] Within a general partnership, an interest in the business entity may constitute a security in situations in which the parties leave so little power in the hands of the partner that the internal distribution of power is effectively similar to that of a limited partnership.[157] That is, the partner must be completely dependent upon the ability of the promoter or manager in carrying out operations, or the partner cannot meaningfully exercise the powers of a general partner in a partnership.[158]

The mining pool arrangement may default to a general partnership entity status. The IRS has taken the view that bitcoin mining is a form of self-employment.[159] Pursuant to partnership law, two or more individuals working together with the intent to share the proceeds of that effort constitutes a partnership.[160] As such, when individual miners work in concert to create value that will be shared among the various members, the default relationship is a general partnership. The question then becomes, does the arrangement between individual participants and the mining pool constitute a security under law?

---

[156] *Williamson*, 645 F.2d at 421.
[157] *Id*.
[158] *See supra* text accompanying notes 130–33.
[159] Notice 2014-21, 2014-16 I.R.B. 938–40 ("If a taxpayer's 'mining' of virtual currency constitutes a trade or business, and . . . is not undertaken . . .as an employee, the net earnings from self-employment . . . resulting from those activities constitute self-employment income and are subject to the self-employment tax.").
[160] UPA at § 202, Cmt. 1.

As discussed, an individual miner involved in a bitcoin mining pool depends heavily upon the pool manager to aggregate work product from all of the miners and convert that work product into value via the bitcoin network.[161] The arrangement is such that it leaves the pool participant with no ability to exercise any power or authority.[162] In some cases, the partner may also be completely dependent upon the actions of the pool promoter in the verification process that she could not otherwise undertake a successful mining activity.[163] Either this level of dependence upon the pool manager or the lack of available control to the pool participant, individually, is likely sufficient to qualify under the *Williamson* Test.[164]

D. Legal Effect of Securities Regulation on Bitcoin Mining

If bitcoin mining pools are deemed to be securities, a full range of regulatory considerations would be triggered, beginning with the registration and disclosure requirements of the 1933 Act.[165] Because the primary purpose of the 1933 Act is to provide potential investors with material information of securities offerings and to prevent unfair practices by those involved in selling securities, the primary burden on those organizing and selling interests in bitcoin mining pools would be to register the offering. To avoid this imposition, the issuers

---

161 *See supra* text accompanying notes 35–45.
162 *See supra* text accompanying notes 35–45.
163 *See supra* text accompanying notes 35–45.
164 *See supra* text accompanying notes 132-35.
165 Securities Act of 1933, 15 U.S.C. § 77b(a)(3) (2014) (outlining the method of registering securities with the SEC).

would need to qualify for one of the many exemptions under the act.

1. Registration

The essence of the registration process is disclosure.[166] That is, the 1933 Act does not require securities arrangements to be profitable, and the SEC is not tasked with evaluating the worth of the offerings.[167] As long as investors have enough information to make informed decisions, they are free to do with their money what they will. In order to achieve adequate disclosure, those involved in selling interests in bitcoin mining pools would be required to file a Form S-1[168] with the SEC. The form requires the disclosure of a wide range of information, including, *inter alia*, the nature of the business, the management and compensation structure, the pool's assets, and the pool's competitors.[169] The form would also require that

---

[166] *See* The Laws that Govern the Securities Industry, U.S. Sec. & Exch. Comm'n, http://www.sec.gov/about/laws.shtml (last visited Jan. 19, 2015) (noting that the primary purpose of the Securities Act was to "require that investors receive financial and other significant information concerning securities being offered for public sale; and [to] prohibit deceit, misrepresentations, and other fraud in the sale of securities").

[167] *Id*. ("This information enables investors, not the government, to make informed judgments about whether to purchase a company's securities. While the SEC requires that the information provided be accurate, it does not guarantee it.").

[168] 17 C.F.R. § 239.11 (2014).

[169] S.E.C. FORM S-1, REGISTRATION STATEMENT UNDER THE SECURITIES ACT OF 1933, *available at* http://www.sec.gov/about/forms/forms-1.pdf (last visited Jan. 19, 2015). The requirement that registrants release information about executive and director compensation was a result of amendments the SEC made regarding their disclosure rules in 1992 and again in 2006. *See* Jennifer S. Martin, *The House of Mouse and Beyond: Assessing the SEC's Efforts to Regulate Executive Compensation*, 32 DEL. J. CORP. L. 481, 490–92 (2007) (outlining the SEC's efforts to regulate executive and director compensation from 1933 through 2006).

the mining pool disclose substantive information about the investment opportunity being offered and how it relates to any other capital securities of the mining pool.[170] Finally, the mining pool would be obligated to publish audited financial statements as part of the registration process.[171]

In addition to making the required filings with the SEC, the mining pool would also be tasked with issuing a prospectus—a document made available to potential investors—containing much of the information required on the Form S-1.[172] The Form S-1 and the prospectus would be available for public inspection almost simultaneously with their arrival at the SEC.[173] Without qualifying for a special exception, the mining pool would still be legally required to wait a full 20 days before being allowed to formally sell interests to investors.[174]

Adding a layer of complexity, the 1934 Securities Exchange Act ("1934 Act") contains its own set of registration rules that may be imposed upon issuers.[175] Until 1982, obligations imposed by these two acts were treated as unrelated and required seemingly duplicative work for registrants. It was in that year, however, that the SEC adopted an approach that allows certain issuers to combine many or all of the disclosures

---

[170] FORM S-1, *supra* note 169.
[171] Regulation S-X, 17 C.F.R. Part 210; *see also* FORM S-1 *supra* note 169, at Item 11(e), (requiring inclusion of financial statements that comply with Regulation S-X).
[172] 15 U.S.C. § 77b(a)(10) (2014).
[173] *See* U.S. Sec. & Exch. Comm'n, *supra* note 166.
[174] 15 U.S.C. § 77h(a). The SEC has the discretion to shorten the 20-day waiting period. *Id*. It also may extend the period if it requires additional information from the issuers. *Id*. § 77h(b).
[175] 15 U.S.C. § 78l (2014).

into the same filing.[176] The test for which issuers may combine parts or all of their filings generally hinges on how seasoned they are—*i.e.*, how experienced the issuer is with the filing process.[177]

While the 1982 amendments may not be overly helpful to mining pools, who often have not been organized long enough to be eligible for "seasoned" status with the SEC, the agency amended its rules again in 1992. These revisions were designed to aid small businesses that intend to offer their investment products for trade in the public markets.[178] While it is unknown the propensity of mining pools to seek access to the public markets, many would meet the definition of a "smaller reporting company" or a "small business issuer" under the rules, which would trigger less stringent reporting requirements.[179]

---

[176] *See* Securities Act Release No. 6385, [1981-1982 Transfer Binder] FED. SEC. L. REP. (CCH) P83,111, at 84,947 (Mar. 3, 1982); Securities Act Release No. 6383, [Accounting Series Releases Transfer Binder] FED. SEC. L. REP. (CCH) P72,328, at 62,990 (Mar. 3, 1982); Securities Act Release No. 6331, [1981-1982 Transfer Binder] FED. SEC. L. REP. (CCH) P83,016, at 84,477 (Aug. 6, 1981); Securities Act Release No. 6235, [1980 Transfer Binder] FED. SEC. L. REP. (CCH) P82,649, at 83,482 (Sept. 2, 1980). *See also* Manning Gilbert Warren III, *A Review of Regulation D: The Present Exemption for Limited Offerings Under the Securities Act of 1933*, 33 Am. U.L. Rev. 355, n. 53 (Winter 1984) (outlining integration of 1933 and 1394 Act disclosures as a result of 1982 amendments).

[177] *See* Joel Seligman, *The Obsolescence of Wall Street: A Contextual Approach to the Evolving Structure of Federal Securities Regulation,* 93 MICH. L. REV. 649, 687-96 (1995) (providing an overview of the "integrated disclosure system" available to "seasoned investors").

[178] Securities Act Release No. 6949, 7 Fed. Sec. L. Rep. (CCH) P 72,439, at 62,166 (July 30, 1992)

[179] An initial public offering of a "small business" or, after February 4, 2008, of a "smaller reporting company," is subject to less stringent disclosure requirements than other issuers. *See* Changeover to the SEC's

Perhaps even more helpful to a mining pool would be revisions to the registration process that came from the Jumpstart Our Business Startup Act of 2012 (JOBS Act).[180] This act offers an easier registration process for "emerging growth companies."[181] In addition, this act authorizes covered businesses to begin communicating with certain investors prior to filing Form S-1.[182] This would allow qualifying mining pools to communicate with sophisticated investors before initiating the cumbersome registration process in order to guage whether or not there is a market for their anticipated offering.

2. Exemptions

As the previous section explains, the registration process for securities issuers involves time and expense. For mining pools, which are currently relatively small operations in

---

New Smaller Reporting Company System by Small Business Issuers and Non-Accelerated Filer Companies: A Small Entity Compliance Guide, *available at* http://www.sec.gov/info/smallbus/-secg/smrepcosysguid.pdf. A "smaller reporting company" if the firm (1) has "a common equity public float of less than $75 million or (2) [is] unable to calculate their public float and have annual revenue of $50 million or less, upon entering the [SEC] system." *Id*. at 2. In contrast, under pre-2008 standards, an issuer qualified as a "small business issuer" if it had "(1) less than $25 million in public float and (2) less than $25 million in annual revenue." *Id*.

[180] Jumpstart Our Business Startups Act ("JOBS Act"), Pub. L. No. 112-106, 126 Stat. 315 (2012) (codified in scattered sections of 15 U.S.C.).

[181] *See* JOBS Act § 101 (outlining the requirements for qualification as an "emerging growth company"). For an in-depth treatment of the registration process for emerging growth companies under the changes brought about as a result of the JOBS Act, see James E. Bitter and Todd B. Skelton, *Reforms for Hire: The JOBS Act Legislation*, 14 TRANSACTIONS: TENN. J. BUS. L. 13, 27-33 (2012).

[182] JOBS Act § 105(c). The investor must be a qualified institutional buyer or an accredited investor. *Id*. *See also* Bitter and Skelton, *supra* note 181, at 29.

terms of capital and revenue, such an expense might prove crippling. This is so even with the aid of the SEC's revised integrated disclosure rules and the JOBS Act.[183] While these provisions lessen the burdens of registration and disclosure, they do not eliminate them. Congress, however, recognized the need to allow small and emerging businesses some means of escaping the registration process; thus, the 1933 Act allows for certain transactions to be completely exempt from the statutory requirements.[184]

The first series of exemptions are housed under Regulation D and include three different types of offerings that are excused from the registration process.[185] Regulation D exempts transactions that are limited in terms of the amount of money involved or in the types of investors being solicited. First, any mining pool that purports to sell no more than $1M worth of interests in any 12 month period will be excused from the registration process under Rule 504.[186] All that is required

---

[183] *See* Bitter and Skelton, *supra* note 181, at 15 ("In small-dollar-value offerings of securities, 'accounting, legal, and other expenses can easily exceed $50,000 . . . .' Such amounts are burdensome, especially as 'relative to the total yield from a small offering,' especially when 'relative, not absolute, offering expenses . . . are [most] important.'") (citing Rutherford B. Campbell, Jr., *Regulation A: Small Businesses' Search For "A Moderate Capital,"* 31 DEL. J. CORP. L. 77, 90 (2006).) .

[184] 15 U.S.C. § 77d (2014). The 1933 Act also prescribes certain securities as exempt from the registration requirements, see 15 U.S.C. § 77c (2014), but interests in mining pools do not fit any of the enumerated securities listed by the act as being exempt.

[185] *See* 17 C.F.R. §§ 230.501-08 (2014). Regulation D now consists of Rules 501 through 508. *Id*. Rules 501 through 503 and Rules 507 through 508 are general rules of support for the exemptions found in Rules 504 through 506.

[186] 17 C.F.R. § 230.504 (2014). This rule applies to private, noninvestment firms. Further, if the offering is registered under state law (or exempted therefrom) the rule permits general solicitations and allows unrestricted re-sales of the interests.

is that the mining pool notify the SEC of its sales.[187] In other words, no Form S-1 must be filed, no prospectus needs to be given to investors, and no independently audited financial statements must be on display. Second, mining pools may raise a significantly greater amount—up to $5M—and still qualify for exemption under Regulation D's Rule 505 with a few additional restrictions.[188] The third exemption under Regulation D, Rule 506, has nothing to do with the dollar amount that is being raised by the issuer but rather deals with who is purchasing the security interest.[189] Under this safe-harbor rule, a mining pool would be allowed to sell interests to an unlimited number of accredited investors[190] and up to 35 non-accredited investors.[191]

Section 4(a)(6) of the 1933 Act offers a relatively new exemption that may be of intrigue to mining pools due to the technological nature of the bitcoin mining process.[192] Known as the "crowdfunding" exemption, it allows issuers to raise funds over the internet from a broad base of investors.[193] Under Section 4(a)(6), a mining pool would be able to raise $1M per

[187] *Id*.
[188] 17 C.F.R. § 230.505 (2014). Unlike Rule 504, Rule 505 prohibits advertising and most solicitation. It also disallows more than 35 non-accredited investors from buying an interest.
[189] 17 C.F.R. § 230.506 (2014).
[190] *Id*. The term "accredited investor" is defined in 17 C.F.R. § 230.501 (2014).
[191] 17 C.F.R. § 230.506.
[192] 15 U.S.C. § 77d(a)(6) (2014).
[193] *Id*. The Section 4(a)(6) exemption was added to the 1933 Act as a result of the 2012 JOBS Act. JOBS Act § 302(b). For more information on crowdfunding, see http://www.nlcfa.org/crowdfund-101.html.

year[194] with minimal disclosures to the SEC and potential investors.[195]

The final two options for mining pools wishing to avoid the involvement and expense of registration offer an additional advantage over the Regulation D and Section 4(a)(6) exemptions. Sales made pursuant to Regulation A[196] or Section 3(a)(11)[197] are made without restriction—*i.e.*, the original purchasers are largely free to transfer their interests to third parties. A mining pool may avail itself to the protections of Regulation A if they cap their issuance at $5M annually.[198] The regulation still requires the submission of an "offering statement" with the SEC and an "offering circular" with potential investors, but these documents are significantly less burdensome to complete than the registration statements and prospectuses required to be completed for non-exempt transactions.[199] Further, audited financial statements are not required to be created under Regulation A.[200]

---

[194] 15 U.S.C. § 77d(a)(6). This amount is adjusted for inflation under the terms of the statute.
[195] *Id*.
[196] 17 C.F.R. §§ 230.251–.263 (2014).
[197] 15 U.S.C. § 77c(a)(11) (2014) (exempting "[a]ny security which is a part of an issue offered and sold only to persons resident within a single State or Territory, where the issuer of such security is a person resident and doing business within or, if a corporation, incorporated by and doing business within, such State or Territory").
[198] 17 C.F.R. § 230.251(b) (2014).
[199] 17 C.F.R. §§ 230.251–.252 (2014).
[200] *See* Harold S. Bloomenthal & Samuel Wolff, SECURITIES AND FEDERAL CORPORATE LAW § 6:43 (2d ed. 2013) (explaining that audited financial statements are not required to be prepared and submitted for issuances not exceeding $5M) (citing SECURITIES AND EXCHANGE COMMISSION, FORM 1-A, REGULATION A OFFERING STATEMENT UNDER THE SECURITIES

The intrastate transaction exemption under Section 3(a)(11), on the other hand, is available regardless of dollar amount or of investor type. It depends solely on all offerrees being located within the same state as the issuer.[201] Thus, a mining pool located in San Francisco would be free to sell interests to an unlimited number of passive investors from San Deigo to Berkeley for any amount. There is room for caution, however, in that the SEC interprets this rule in the strictest sense.[202] To provide assurance to issuers relying on this exemption, the agency published Rule 147, which provides a safe-harbor.[203] In essence, our San Francisco mining pool would need to assure that at least 80% of its assets and revenues came from California, and it would further need to assure that no resales of its interests took place to nonresidents for a nine month period after the initial sale.[204]

3. Liability

To underscore the importance of seeking an exemption, the 1933 Act provides for austere sanctions for failure to comply with the strict requirements of the registration process. First, Section 12(a)(1) of the 1933 Act creates civil liability for selling a security without the required registration.[205] It also

---

ACT OF 1933, *available at* https://www.sec.gov/about/forms/form1-a.pdf. (last visited Jan. 25, 2015)).

[201] 15 U.S.C. § 77c(a)(11) (2014).

[202] *See, e.g.*, Bryan Vaaler, *Financing a Small Business in Mississippi: A Practitioner's Guide to Federal and State Securities Exemptions Part II,* 63 MISS. L.J. 267, 306-11 (1994) (outlining intrastate exemption and the SEC and the courts' historical tendencies to read the exemption narrowly).

[203] 17 CFR § 230.147 (2014).

[204] *Id*. To assure that no re-sales occur to non-residents, the rule states that issuers take precautions such as placing a notation on the certificate of interest or securing an official proof of residence from each investor.

[205] 15 U.S.C. § 77l(a)(1) (2014).

covers sales made without the issuance of a prospectus or with the issuance of an inaccurate or non-current prospectus.[206] Next, Section 11 of the 1933 Act penalizes false or misleading statements (or material omissions) contained in any registration statement.[207] This provision covers far more than just the seller, extending liability to directors, owners, any professional who certified any part of the registration statement, any signatory on the statement, and all underwriters.[208] While Section 12(a)(1) does not offer the seller any defense for an unregistered sale, Section 11 contains a due diligence defense that hinges on the party's belief in the truth of the registration statements as well as the reasonableness of that belief.[209] Similar to Section 11 is Section 12(a)(2), which imposes liablity on sellers who make material misstatements in a prospectus or in any oral communication to a purchaser of a security.[210] Finally, Section 17(a) is an anti-fraud provision that empowers the SEC to pursue an enforcement action for interstate offers or sales that include certain types of fraud that are enumerated in the section.[211] In addition to the civil penalties provided for in the 1933 Act, there are also criminal sanctions provided for in the act, which allow for imprisonment and monetary fines.[212]

---

[206] *Id*.
[207] 15 U.S.C. § 77k (2014). Rule 405 explains that the word "material" is intended to limit "the information required to those matters to which there is a substantial likelihood that a reasonable investor would attach importance in determining whether to purchase the security registered." 17 C.F.R. § 230.405 (2014).
[208] *Id*. As a general rule, those liable under Section 11 are jointly and severally liable. § 77k(f).
[209] 15 U.S.C. § 77k(b)(3), (c).
[210] 15 U.S.C. § 77l(a)(2) (2014). The seller will avoid liability to the extent it is shown that part of the purchaser's damages resulted from something different than the untrue communication.
[211] 15 U.S.C. § 77q (2014).
[212] 15 U.S.C. § 77x (2014).

IV. CONCLUSION

The use and acceptance of bitcoin has grown exponentially over the past several years, with the bitcoin economy now representing a multi-billion dollar enterprise. To date, there has been little regulation of bitcoin. As more individuals begin to invest in bitcoin mining pools, the risk of these individuals being taken advantage of or falling victim to fraud increases. Rather than developing a separate regulatory scheme for bitcoin and similar virtual currencies, the United States can and should apply federal securities laws to regulate investors' interests in bitcoin mining pools. Specifically, those who invest in bitcoin mining pools should benefit from the disclosure requirements under the 1933 Act, as these investments fall squarely within the *Howey* Test for investment contracts. These investors (1) make an investment of money (2) into a common enterprise (3) with the expectation of profits (4) that are derived predominantly from the efforts of others, namely those actively involved in the bitcoin mining process. As such, the investments should be regulated under the federal securities laws.

PEER-REVIEWED JOURNAL ON THE INTERNET

Volume 20, Number 12 - 7 December 2015

PEER-REVIEWED JOURNAL ON THE INTERNET

Blockchains and Bitcoin: Regulatory responses to cryptocurrencies

Andres Guadamuz and Chris Marsden

Abstract

This paper examines Bitcoin from a legal and regulatory perspective, answering several important questions.

We begin by explaining what Bitcoin is, and why it matters. We describe problems with Bitcoin as a method of implementing a cryptocurrency. This introduction to cryptocurrencies allows us eventually to ask the inevitable question: is it legal? What are the regulatory responses to the currency? Can it be regulated?

We make clear why virtual currencies are of interest, how self-regulation has failed, and what useful lessons can be learned. Finally, we produce useful and semi-permanent findings into the usefulness of virtual currencies in general, blockchains as a means of mining currency, and the profundity of Bitcoin as compared with the development of block chain technologies. We conclude that though Bitcoin may be the equivalent of Second Life a decade later, so blockchains may be the equivalent of Web 2.0 social networks, a truly transformative social technology.

Contents

---

1. Introduction: The hype about Bitcoin as a cryptocurrency

In 2008, the developed world banking system almost collapsed and had to be rescued by sovereign governments via takeovers of bad banks with bad loans, and the printing of money to loan to major banks, whether rescued or surviving. In the long recession of 2008 to 2014, governments supported their economies with a variety of means. With close to zero inflation and interest rates, governments had to find ways to stimulate some economic growth. They fell on three main solutions: limited stimulus via infrastructure spending, such as the American Reinvestment and Recovery Act of 2009; support for ICT-enabled, often environmentally sustainable industries to create new 'virtual' growth in the digital economy [1], some of it linked to the first option [2]; quantitative easing or the printing of money given to banks at low interest rates. Mason reports that the "[United States of] America and Britain did it first, in early 2009; Japan waded in massively in 2012 and the Eurozone finally did it, in the teeth of German resistance, in January this year." [3]

Reactions to the rescuing of banks were mixed, with many of those opposed to the policy either resorting to investment in commodities and bullion, for instance property and gold (which rose in value 350 percent 2006–12, and is still double 2006 levels at over US$1,100/ounce). Others chose a more radical path. Iceland bankrupted its banks and massively devalued its currency [4]. It then adopted a series of policies that alienated the population in a severe recession. In late 2015, the largest party by popular support is the Icelandic Pirate Party [5], which proposes far wider use of virtual currencies which would not rely on sovereign support. We should also note that throughout the years of recession (most developed economies regained 2008 levels of income after six years, with the notable exception of Greece and Iceland), the wealthiest quartile of the population invested massively in the "Apple economy", spending sovereign currency on a billion iPhones and other consumer electronics and services such as NetFlix movies and Amazon purchases. Rejection of the mass consumer economic model funded by debt is by no means universal or even a majority view.

In January 2011, an aspiring entrepreneur called Ross Ulbricht created an online marketplace called Silk Road [6]. This was not just another electronic commerce Web site, Silk Road was unique in almost all of its features. First, it was not available on the normal Web. It existed in an encrypted and secretive part of the Internet called the 'dark Net' [7]. Second, it offered a range of illegal merchandise not found on eBay or Amazon, mostly drugs, catering to discerning users by offering customer reviews and vendor ratings. Third, the

Silk Road was able to operate because it used a new virtual currency called Bitcoin that allowed users to remain anonymous and conduct transactions with little fear of interference by law enforcement.

While the Silk Road was eventually shut down and its creator arrested and convicted [8], the publicity that the case garnered for Bitcoin helped to establish it in the public's imagination as a powerful sign of the probabilities of the digital economy. The currency has even transcended the financial pages to be featured in popular television shows like *The Good Wife, Almost Human* and *The Simpsons*. Even the famous Winklevoss twins, of Facebook fame, have become heavy investors. Academics have published many social science papers about Bitcoin since 2011, with increasing regularity: six by the end of 2012, 19 in 2013 and 135 since the beginning of 2014 until August 2015 [9]. It is not merely an academic fashion: many books have been published in the period since we published a working paper on which this work is based [10], from the how-to-get-rich-quick variety [11] to the revolutionary [12] and its anti-thesis [13] to regulatory [14] and even academic [15]. Inevitably, a 'burst the bubble' anti-hype book concludes that: "There are fewer people using bitcoins to buy goods and services than there are members enrolled in Kuwait Airways frequent flyer program. And yet ... the blockchain technology behind bitcoin, is brilliant and will absolutely change the world." [16] We shared that conclusion in 2014 and continue to do so today.

This paper will look at Bitcoin from a legal and regulatory perspective, answering several important questions. We begin by explaining what Bitcoin is, and why it matters. In the following section, we explain problems with Bitcoin as a method of implementing a cryptocurrency. We are aware that the introductory section may seem extensive, and that including a very detailed description of currencies and Bitcoin may seem basic at this level. This is done on purpose, because in our experience whenever there is talk of Bitcoin and blockchains, non-technical audiences tend to miss the importance of some developments because they do not understand the basics. It is one of the goals of this article to be able to act as an easy introduction to cryptocurrencies. We ask the inevitable question for lawyers: is it legal? What are the regulatory responses to the currency? Can it be regulated? We explain why virtual currencies are of interest, how self-regulation has failed, and what useful lessons can be learned. Finally, we produce useful and semi-permanent findings into the usefulness of virtual currencies in general, block chains as a means of mining currency, and the profundity of 'media darling' currency Bitcoin as compared with the development of blockchain technologies [17]. We conclude that though Bitcoin may be the equivalent of Second Life, so blockchains may be the equivalent of Web 2.0 social networks, a truly transformative social technology.

2. Introduction to Bitcoin

2.1. Virtual currencies

There is a voluminous literature on regulation of virtual economies [18], virtual communities [19] and a fast emerging literature on Bitcoin itself [20]. From Facebook Credits to Bitcoin (BTC), virtual currencies have had a bumpy evolution. Virtual currencies are wildly successful in their respective in-game economies, they are used by millions to buy goods and services in limited virtual environments, and it has been proven that people will pay real cash to boost their online content [21]. Amazon has announced that it will be launching its own virtual currency for their Kindle app store, Amazon Coins. Amazon Coins will almost certainly be used exclusively within the Kindle environment to buy content for the Kindle, such as books, music, movies and TV shows. This replicates earlier uses of reward schemes to regular shoppers, from air miles and airline rewards, to Green Shield stamps in the 1960s and 1970s, to the Cooperative Society's dividends and stamps, and the now-ubiquitous reward programmes of online merchants.

Virtual communities can create social networks but also valuable goods and services for other users [22]. This value is generally exchangeable for real world currencies, as in the largest role-player community World of Warcraft with an economy measurable in the billions of U.S. dollars, though the largest social network Facebook uses sovereign currencies as do its third party games developers [23]. Most virtual community developers have historically claimed ownership of everything hosted in their servers, making them the 'sovereign' in the community [24]. This may include items with real-world value, such as virtual currency converted into real cash by the means of some exchange, as when players of online games purchase gold and in-game currencies from Chinese 'gold' farmers, creating tools for World of Warcraft and other virtual communities [25]. Some virtual communities have gone further, developing virtual currencies that can be accepted in other communities.

Bitcoin has taken a further step, as it is a virtual currency that claims to be tradable in exactly the same fashion as sovereign currencies, yet without a sovereign. We now explain the basics of currencies before examining Bitcoin's challenges to that model.

2.2. Currency basics

Bitcoin is a non-fiat cryptographic electronic payment system that purports to be the world's first cryptocurrency. In other words, it is a peer-to-peer, client-based, completely distributed currency that does not depend on centralised issuing bodies (a 'sovereign') to operate. The value is created by users, and the operation is distributed using an open source client that can be installed on any computer or mobile device. In order to better understand Bitcoin, we will discuss currencies in general, and electronic currencies specifically.

Payment systems in general, and currency specifically, depend on value. Value is simply the desirability that someone allocates to something, generally material items according to our needs, such as food and shelter, or according to their scarcity, such as gold; we also give value to energy in the shape of

labour. Finally, we value intangibles, such as experience, knowledge, creativity and know-how [26].

Currencies were invented as a means to transfer value. Initially, this was done through barter, and then people started allocating value to coins using metals that were considered inherently valuable for their scarcity. In the Renaissance in Europe [27], as coins became unwieldy, a more flexible system of value embedded in paper money was devised in order to make transactions easier, as carrying gold and silver bullion was insecure and expensive [28]. The first paper notes worked as a promise to give the bearer the equivalent value in metal to the one inscribed on the document. Money therefore relied on the idea that the issuer had metal reserves that could be redeemed at any time, hence giving value to a given currency. The problem with this system, called the gold or silver standard [29], is that it placed a limit on the amount of money that could be exchanged at any given time by the issuer to that which could be allocated to metal reserves, therefore creating an upper limit to the size of the economy that was equal to the available metal (expansion of empire was often motivated and financed in part by the desire to gain gold and silver reserves, as for the Spanish and Portuguese in South America and British in South Africa). When a country needed to issue more money than it had in metal reserves, such as during time of war, this could result in devaluation, as people would not trust that there were reserves that supported the money.

During the twentieth century the gold standard was abandoned, and a new monetary system was put in place that uses a country's wealth and economic trustworthiness as the basis for value. This is what is known as fiat [30] money. Modern fiat currencies have value based on the economic strength of the issuer. In some libertarian and anarchist circles, it is said that fiat money does not have any inherent value, but this fails to recognise that neither does the gold standard [31]. Gold does not have intrinsic value; under the right circumstances gold could be valueless except as an industrial input. In fact, there is no such thing as inherent value; all value is dependent on circumstances. The value in fiat money arises from the law, the currency has the support of the government as sovereign, and therefore, it is supported by the economy of the territory where it is accepted. Trusted governments support strongly valued currencies, though governments permitting hyperinflation can destroy that trust.

2.3. Bitcoin

Bitcoin was developed in 2008 as a concept by an anonymous developer going by the pseudonym of Satoshi Nakamoto, who posted a paper detailing the currency to a cryptography mailing list [32]. The paper details a decentralised system with no issuing authority that would serve as both a means of exchange but also as an anonymous and fully open log of all transactions (known as the blockchain). People running a client that would "mine" value by verifying transactions would create the value, which encourages users to allocate processor time to confirm trades.

The paper gained some traction in cryptology circles, and it was coupled with the anonymous registration of the Bitcon.org domain, as well as the release on 9 January 2009 of the first version of the Bitcoin client [33]. The currency continued to become more popular, but it was not until the creation of the Silk Road in 2011 that it achieved more mainstream notice [34].

Bitcoin was devised as a non-fiat currency; in other words, its proponents claim that it has “real” value. The value arises from computing power, that is, the only way to create new coins is by allocating distributed CPU power through computer programs named “miners”. The miners create a block after a period of time that is worth an ever-decreasing amount of bitcoins in order to ensure scarcity. Each bitcoin consists of 100 million smaller units, with each unit called a satoshi. The operations performed to mine are precisely to authenticate other transactions, so the system both creates value and authenticates itself, an elegant and simple solution that is one of the appealing aspects of the currency. Once created, each Bitcoin (or 100 million satoshis) exists as a cryptographic address that is part of the block that gave birth to it. The person who mined the coin owns the address, and can transfer it by sending value to a another address, which is a “wallet” file stored in a computer. The blockchain is the public record of all transactions.

Another way of looking at the currency is that Bitcoin is simply allocating value arbitrarily to a program that performs the mathematical equations necessary to support the creation of a bitcoin. It is a self-referential and circular currency, and its only value is that which people give it, just like fiat money, but with faith placed in computer programming, not sovereign states.

Why do people use Bitcoin and dedicate computing resources to mine them? One obvious element would be profit, but even before mining was profitable, there were thousands of people dedicating resources and efforts to the currency. Any visit to a Bitcoin discussion forum provides evidence that an important core of the BTC community consists of libertarian types of all stripes, from those who want to see the end of all fiat currencies, to slightly more moderate and pragmatic supporters [35]. A libertarian tinge permeates some of the most vocal currency’s proponents, who attack established fiat currencies, which they see as anathema to the system of value established by the gold standard. However, most seem to accept that coexistence will be prevalent.

A more nuanced picture of the user base is beginning to emerge. Liu conducted a survey of over a thousand cryptocurrency enthusiasts in various Web sites, and found that the average BTC user is a 32-year-old libertarian male, motivated by curiosity, profit and politics [36]. Yelowitz and Wilson conducted a large study using Google Trends data from the United States, and found that computer science and illegal activity were some of the most prevalent topics linked with Bitcoin, with less correlation to political discourse and investment [37].

Bitcoin adoption may be motivated by a various number of features, including transparency, politics, anonymity and its use in illegal activities. Studying

community dynamics is therefore made much more difficult than even such pseudonymous or avatar based communities as Habbo Hotel, World of Warcraft or Second Life. The ethical implications of studying such communities raise similar problems as those of Tor, Anonymous [38], Lulzsec and other anonymous hacker communities [39]. Journalistic accounts of BitCoin markets are largely subject to sensationalism, hype and inaccuracy, even more so than in the earlier hype cycle for Second Life, exacerbated by the first issue of anonymity. Ideally, a decentralized currency should be politically neutral and strive to be efficient. Any ’revolutionary effects‘ would be caused by its success, not as part of a plan to bring about a libertarian utopia [40].

2.4. Scarcity and economic value in Bitcoin

An important part of the concept behind Bitcoin is that it has built-in scarcity because mining for coins becomes more difficult as time goes by and the market grows [41]. The algorithms that produce new BTC coins increase the amount of processing power necessary to create each new block, so producing new coins is more difficult. This difficulty is built into the system to in order to keep the total amount of Bitcoins at a maximum of 21 million.

The first block ”mined“ was at difficulty 1, and this is known as the genesis block [42]. By June 2011, there were 131,301 blocks, making a total BTC of 6,560,000, and a difficulty of 877,227. In June 2014, there were 303,162 blocks with a total 12,800,000 BTC in existence, and a difficulty of over 10 billion. At the time of writing (June 2015), there were 359,657 blocks and just over 14 million BTC had been mined, with a difficulty of over 47.5 billion.

That means, making a new block is more than 47 billion times more difficult than it was for the initial block, and four times more difficult than it was exactly one year before. This difficulty will only go up, so an individual cannot hope to have the processing power to develop new coins, and this can only be done currently through pool mining CPU resources [43].

While this model is trying to replicate scarcity in the market, it acts as a punishing disadvantage for late adopters, and means that early adopters have market power if they hoarded coins. This may have regulatory repercussions in the future.

Because late adopters and interested individuals cannot hope to mine new coins, the BTC economy relies on users buying bitcoins with fiat currencies through exchanges. These are companies that hold bitcoins and are willing to sell them at an exchange rate. In other words, intermediaries will accept your “normal” currency and exchange it into bitcoins, and vice versa [44]. For most large part of its early history, Bitcoin relied very heavily on one intermediary, a Tokyo-based company called Mt. Gox. There have been dozens of exchanges, as in theory literally anyone could set up their own firm. Mt. Gox was famous for having started out as an outfit to trade “Magic the Gathering” cards, but then evolved to be the largest exchange. Ron and Shamir found that Mt. Gox had intervened in 90 percent of all Bitcoin transactions ever recorded

[45]. In the same study, they found that there is some large accumulation of the bulk of Bitcoin activity, for example, one single user (Mt. Gox itself) had 156,722 different addresses. This level of centrality is not good for a supposedly decentralized currency. Many blips in price prior to the crash were caused precisely by DDoS attacks against Mt. Gox [46]. As we will discuss later, Mt. Gox became embroiled in serious fraud accusations. Similarly, such reliance makes the entire system less resilient and prone to catastrophic failures, but we will analyse those issues later.

2.5. Altcoins

Bitcoin has undoubtedly become the most talked about cryptocurrency, but it is easy to forget that it began mostly as a proof of concept. Because the software is completely open source [47], any developer can download it, modify it and create her own version of the software. This capability has led to an explosion of alternative bitcoin implementations, popularly known as altcoins. There are no limits to the number of altcoins that can be released, but in practice there are a few dozen real alternatives that implement minor or major changes; these are known as forks.

There is no single reason why a developer should fork the original code and create their own version. Some may do it to improve the code, to create better security, to modify some of the existing parameters, as a joke, or to attempt to convert altcoins into bitcoins [48].

Some of the most popular implementations are:

- *IxCoin (IXC):* The International eXchange Coin [49] is the first Bitcoin clone. It was released in 2011 and it can be mined at the same time as BTC. It also has a limit of 21 million coins, but much shorter mining period (all coins should have been mined in 2015).
- *Namecoin (NMC):* It is one of the most innovative altcoins [50]. It uses Bitcoin to create a decentralised domain name system outside of the existing international system operated by ICANN. The service allows the registration of domain names that cannot be shut down or taken over by law enforcement.
- *Litecoin (LTC):* This is one of the more popular Bitcoin alternatives [51], it was created specifically to fix perceived shortcomings in BTC, and it boasts faster transaction verification times and improved storage efficiency.
- *Ripple (XRP):* In the strict sense, Ripple is not a direct Bitcoin fork [52], but it borrows some of the main ideas of Bitcoin, such as being an open source decentralised ledger. It is a currency, but also it acts as an exchange protocol for existing currencies and altcoins.
- *Dogecoin:* This started as a joke BTC fork in 2013 [53], but quickly became a currency in its own right, with a 2015 estimated market capitalisation of over US$15 million [54], making it the fourth most popular altcoin. The name comes from Doge, the popular Internet meme [55].

- *Bitcoin XT:* This is a very recent and controversial fork [56] to the original Bitcoin source code that adds two main changes, the block size is increased and it removes the need to download the entire blockchain.

2.6. Key benefits

While it can be argued that Bitcoin has become better known in technology circles, at least at the time of writing, it still continues to fall short of wider recognition and dissemination. Even though the currency has achieved a non-negligible market capitalisation of US$3.2 billion in 2015 [57], this is still relatively small [58]. Similarly, the indicators for economic activity in the currency, such as trade volume, have remained relatively small [59]. Bitcoin continues on despite this relative obscurity, and some other problems that will be detailed later in this paper.

There are various problems with existing financial markets and currencies that cryptocurrency is trying to address. Some of the benefits of cryptocurrrency are:

- *Transparency:* One of the key benefits of Bitcoin is that all transactions are publicly available and verifiable in the electronic ledger called the blockchain [60]. This provides an unprecedented level of transparency and peer verification; it is one of the features that transcends currency elements.
- *Security:* Bitcoin uses the 256-bit version of the secure hash algorithm (SHA), an encryption protocol designed by the U.S. National Security Agency. The protocol maintains the integrity of the blockchain, but is also used to sign and secure BTC wallets, providing a mathematical proof that transactions are performed from the owner of the wallet. The signature also prevents the transaction from being altered by anybody once it has been issued [61].
- *Lower transaction costs:* While in theory Bitcoin transactions could be free between all parties, the system usually has transaction fees that vary from one exchange to the other [62]. Usually, the transaction fee will go to the miner (as an incentive to miners), and these transaction fees are a function of difficulty [63]. Even with these fees, Bitcoin still boasts lower transaction costs when compared to other payment methods, with some merchants estimating that the average is at one percent, as opposed to other intermediary clearinghouses such as PayPal and Western Union, which charge from two to four percent [64]. However, it must be noted that some researchers believe that low transaction costs will not sustainable in the future [65].
- *Anonymity:* Bitcoin is theoretically anonymous. A person in possession of BTC in an encrypted wallet can spend it in any service without identification. While the anonymity aspect has clearly made it attractive as a means of payment for illegal goods and services [66], it could be used for less nefarious purposes, such as funding campaigners in authoritarian regimes [67].

- *Resilience:* Bitcoin is a decentralised currency with no central authority and no issuing body. This means that it is resilient to attacks, and in theory it also means that it cannot be brought down [68].
- *Engine for innovation:* While it is easy to ignore some grandiose claims made by some Bitcoin developers, such as the claim that it will destroy fiat currencies, or that it has the potential to combat poverty and oppression [69], it cannot be denied that its creation has given a much needed push towards innovation in the way in which we think about money, financial institutions and centrality. Anything that encourages innovation is to be welcomed.

This list is not exhaustive and only shows some of the most cited benefits of the virtual currency. There are some benefits that are more difficult to quantify. For example, there is little doubt that whatever may happen with Bitcoin, its creation has revolutionised how we think about money, value and payments in general. It is possible to be sceptical of Bitcoin, yet to be awed by its elegance and the ambitious nature of its implementation. Even if it were to disappear tomorrow, it is possible that some applications of the technology will survive. We will deal with these in the next section.

3. Problems with the current implementation

While it is clear that Bitcoin has some attractive features, it also has some serious problems that have translated into it not being adopted in the mainstream. Some of the main concerns are listed below, in no particular order.

3.1. Lack of transparency

A main selling points of Bitcoin is transparency. The client itself is open source and all transactions are open to scrutiny because all transactions must be verified by the whole, so it is possible to look at each individual transaction in the public blockchain to scrutinise outgoing and incoming wallet addresses. The addresses do not identify the person, only the possessor of the key that unlocks the address. This makes it both anonymous and transparent at the same time, a feature that explains Bitcoin's popularity with the technical community.

However, this transparency is in practice limited when one considers the currency's origins. Satoshi Nakamoto, the fabled originator of the scheme, remains anonymous to this day. It is a matter of record that Bitcoin was created by a member (or members) of a cryptography mailing list using Nakamoto as a pseudonym. Some suspect that Bitcoin operates in a manner similar to a Ponzi scheme, where those early adopters at the top amassed large BTC stocks, so that the resulting coins can be easily manipulated. The barrier-to-entry is not only physically high (difficulty increases with time), but also a

psychological investment for anyone who understands how easy it would for an early adopter to maliciously manipulate the market.

The fact that some investors have amassed large BTC fortunes is an indication that this could be used to leverage the market. There have been several examples of possible market manipulation, with sudden large volumes in trade used to shift the price up or down [70]. There is also growing evidence that bots have been involved in currency-price manipulation on a large scale, with some analysts identifying a trading bot (nicknamed 'Willy') as being potentially responsible for inflating the price until it reached US$1,300 per bitcoin [71].

It seems increasingly indefensible for Satoshi Nakamoto to remain anonymous, particularly given the potential power of early adopters and the creators of the scheme. For such a transparent currency from a technical standpoint, this remains a rather difficult area for outsiders.

3.2. Failing anonymity

Anonymity is one of the biggest selling points for Bitcoin. This was made evident after an article in the *Atlantic* described Silk Road, a site where drugs could be acquired using Bitcoins [72]. BTC's value increased, usage increased and mining rigs were created using supercomputers and graphic cards. Because the currency is encrypted, there is theoretically no method to trace any given transaction to individual users. However, many papers express serious doubts on the much-heralded anonymity present in Bitcoin. Reid and Harrigan [73] warned that Bitcoin's much-touted anonymity was seriously flawed:

> "Many organizations and services such as on-line stores that accept Bitcoins, exchanges, laundry services and mixers have access to identifying information regarding their users, *e.g.*, e-mail addresses, shipping addresses, credit card and bank account details, IP addresses, etc. If any of this information was publicly available, or accessible by, say, law enforcement agencies, then the identities of users involved in related transactions may also be at risk." [74]

As a case study, they used a highly-publicised theft of 25,000 BTCs (with a value at the time of theft of approximately US$500,000). They were able to follow the involved transactions using their network tools, and charted these with high level of accuracy. They concluded that using network analysis and network representation it is possible to map many users to their public keys. Furthermore, an interested party could potentially try to find more information by targeting centralised services, such as exchanges and online wallet services [75].

Ober and Hamacher found that maximum anonymity is simply not possible, and that there are many points in which it would be possible for an 'adversary' to identify a party successfully [76]. This can be achieved because many

addresses are known in advance, such as addresses that originate from popular long-running mining pools. The number of operators in the Bitcoin economy has been increasing as a function of price, but the authors were able to identify some large players, allocating an identity to some BTC public key addresses [77]. It would be possible for an observer to start identifying addresses, continuously updating the list based on incoming transactions, and using merging of coins to identify two separate entities as a single one. Eventually it would be possible to identify large coin owners when they merge their coins.

Furthermore, Bitcoin users usually need to rely on intermediaries in order to purchase bitcoins, and most of these require identifying information to open an account. This data could be used to de-anonymise the user [78]. To respond to these threats, some services have been created that allows users to 'mix' their coins swapping them and changing them from one address to another, providing further anonymity, albeit with mixed results [79].

Bitcoin anonymity ultimately fails because users cannot help but operate in the real world. The arrest of Ross Ulbricht offers an excellent example of someone who had astounding levels of security and anonymity, but was eventually brought down because he made small mistakes that eventually accumulated, making it possible for law enforcement to find him [80]. This is not a problem in itself with BTC, but it serves as a timely reminder that online activity is eventually subject to regulation.

3.3. Instability

Bitcoin has been tremendously unstable throughout its trading history. While generally the overall trend has been upward if we compare today's value with that of four years ago [81], the currency has crashed several times and the price continues to swing up and down repeatedly. During its peak in December 2013, the price reached US$1,147 per 1BTC (higher in some exchanges), only to crash spectacularly to US$522 in just a few days. Needless to say, such instability is one of the reasons why it is very unlikely to be a viable currency. Imagine that you are a merchant who decides to accept BTC, and agree with a buyer to sell at the trading rate when the transaction was initiated. The first problem you would encounter is that the transaction needs to be verified, and as there are more verifications taking place all the time, the process takes longer (about an hour). With wild variations in price, it is possible that you could lose money even before the transaction has been completed. Moreover, even a minor downward swing, which are too common throughout its trading history, could wipe away any profit.

Bitcoin's price has stabilised somewhat in the last year, but it still can suffer swings of up to US$20 in price. This makes it too unstable and seems to be keeping away investors, making it an unreliable means of payment [82]. Price instability could be part of the decentralised nature of the technology. Yglesias argues that it may continue to vary cyclically in price [83]:

> "If everyone's hoarding their Bitcoins, then the network is actually useless. Since it turns out to be useless, you get a crash.

> The funny thing is that once the upward spiral comes to an end, the technological virtues of the Bitcoin platform come to the fore again."

Fiat money is kept stable by all sorts of means, from fiscal policies to centralized decisions about interest rates, with devaluation or revaluation largely managed by central banks and governments to ensure an orderly change of equilibrium. Panics were caused in 2008 with the sudden devaluation of the Swiss franc and Icelandic krona, or in 1998 with the devaluation of the Russian rouble and other currencies. It is possible that stability can only be achieved through centralization. Others have proposed more libertarian methods of creating stability [84], but at the moment there is no solution as long as the currency remains mostly a speculative vehicle, and not so much a currency for paying for goods and services.

3.4. Lack of replicability

In danger of over simplifying a complex issue, Bitcoin is nothing more than the ownership of a cryptographic address. In reality, most bitcoins exist only as files in a computer or mobile device; a wallet file has access to a private key used to secure the money. This creates one of the biggest issues with Bitcoin to date: the ease of losing one. If the wallet file is lost, then the bitcoins it contains are lost forever [85]. There are ways to back up the keys, such as by keeping physical copies off-line and similarly the key files can be backed up. But if a backup fails, the value will be forever lost. It is simply irretrievable unless one breaks the very secure encryption built into the system. The public address still exists, but this can only be accessed by the private key, which has been deleted and it would not be possible to recover the lost coins.

There are indications that there are large numbers of lost coins in the system. Ron and Shamir examined very old "dormant" addresses in the blockchain, and assumed that these were probably lost coins from a time when people were testing the technology and deleted their wallets [86]. The authors calculated the historical number of lost coins to be 1,657,480 bitcoins. Considering the certainty of later losses, the total value of lost coins could very well double that number. Developer John Ratcliff conducted a similar study of the blockchain, and identified a very large number of dormant coins, what he called 'zombie coins', which amount to 30 percent of all the Bitcoins ever mined [87]. While it is difficult to ascertain just how many of these coins are lost, this is evidence of a serious problem for the viability of Bitcoin.

It must be said that missing and lost coins has not been seen as a problem for enthusiasts, as they point out that each BTC is divisible up to eight decimal points. It is also assumed that the fewer BTCs there are, the higher the value. Defenders of Bitcoin also point out that it is possible to lose real money. This seems disingenuous, as the finality of Bitcoin loss is absolute. People tend to know where their wallet is, but are less conscious about files on their computer. Similarly, normal consumers do not keep all their money stashed in one location. The lack of a failsafe when things inevitably go wrong is a serious issue with the scheme.

The solution to this concern is to keep wallets online, a centralized solution that has its own problems, chiefly that one has to rely on unregulated intermediary 'banks' holding a given wallet. Some online wallets have had problems with security and lost coins, not to mention the real possibility of fraud.

3.5. Deflation

Bitcoin is built with scarcity in mind. The idea is that the scarcity will ensure upward valuation of the currency because there is no central bank that can print more money, as the economy requires it. The problem with deflation is that it encourages hoarding, in which case the currency is not being used as intended, namely to exchange goods and services [88]. Moderate inflation is desired in a healthy economy because it encourages investment and spending, as shown in the recent deflationary crises in Japan and the Eurozone. When Bitcoin was experiencing its upward trend, many commentators noted that a rise in value meant that it had entered a hyper-deflationary spiral which made it uniquely unsuitable as a currency because there was no reason to spend BTCs if the price would continue to rise. In the early days of Bitcoin, an individual reportedly spent 10,000 bitcoins to buy a pizza. In a deflationary economy, this person feels that they lost greatly as the currency's value goes up, and would be less willing to part with their currency in the future.

A stable currency abhors deflation, otherwise it ceases acting as a medium of exchange and becomes akin to scarce commodities, such as diamonds. Furthermore, the decentralised nature of Bitcoin makes it uniquely unfit for banking [89], which would further encourage hoarding by individuals.

There is some evidence that hoarding is taking place. Ron and Shamir found that the actual number of BTCs in circulation was considerably smaller than previously thought, with 78 percent of the entire BTC reserve at the time (7,019,100 BTC) placed in "saving" addresses, and only 22 percent of all BTCs created (including those lost) in circulation [90]. This confirms the suspicion that the system encourages hoarding and accumulation, which make it uniquely unsuitable as a currency. A large number of transactions appear to consist of operations between the same owner, where the coins are moved from one address to another. The data strongly indicates that there is considerable ownership concentration in the BTC network. Ron and Shamir found that:

> "Thirty-six percent of all owners received fewer than one BTC (currently worth about US$12) each throughout their lifetime, 52 percent received fewer than 10 BTCs and 88 percent fewer than 100. At the other end of the distribution there are only four owners who received over 800,000 BTCs and 80 owners who received over 400,000." [91]

The list of BTC owners includes a single unidentified user with 2,886,650 coins, or more than a quarter of all BTCs issued so far. This hints at hoarding

by just a few. BTC is not being used as a payment system, but as a commodity where users exchange bitcoins for cash and vice versa.

3.6. Security and BTC theft

Criminal lawyers and investigators have taken a very significant interest in Bitcoin [92]. An aspect of the trust in Bitcoin is its security, touted as a very secure and anonymous method of transferring value from one computer to the other. The currency works by allocating a public cryptographic key to arbitrary units of value held in a non-proprietary client. Because they are public, the keys can be inspected by everyone, but a private key is needed to make the transaction. These units of value are held in “wallets”, small .dat files hosted in the computer. This serves two purposes: as long as the keys are secure, only the wallet’s owner will be able to transfer the bitcoins to make a payment; the keys make transactions anonymous.

As with many things online, theory is often defeated by a combination of greed, laziness, ignorance and simple intermediary failure. As stated earlier, Bitcoin’s cryptography is very strong, so a hacking attack would not be able to break the security. But a hacker doesn’t need to defeat the SHA–256 cryptographic hash in order to remove bitcoins from the wallet, a simple US$5 dollar wrench would suffice [93]. Practice has been bearing this out. For a long time, the Bitcoin client did not encrypt the wallet.dat file itself, which left the currency vulnerable to basic hacking attacks [94]. Similarly, hackers began successfully targeting the exchanges, managing to steal thousands of BTCs [95]. Strong encryption of the scheme does not protect against fraudsters and scam artists. The security issues with Bitcoin are hard to assess, but risk assessment of various aspects of Bitcoin undertaken by NEMODE, a U.K.-based research project, has concluded that there are various security issues with very high risk, such as general security, subversive miner strategies, loss of keys and man-in-the-middle attacks [96].

This is a serious problem with the currency. As exchanges and wallets are the weakest links in the chain, the currency requires some technical knowledge to operate securely, and this could affect average users from adopting the currency. This relative insecurity stands in stark contrast with existing protection given to traditional banking users [97]. The only BTC recourse is reputational: to go online to complain.

Law enforcement is difficult because agencies may simply not understand the technology, not considering it worthy of prosecution. Until there are arrests related to BTC fraud and hacking, serious investors might well decide to stay away from Bitcoin because it simply is not safe enough, as it draws hackers like no other payment system. Bitcoin might therefore be suffering from a lack of regulation, something that could be considered ironic, as one of its selling points is the distributed nature of the network, which makes it difficult to regulate in the first place.

3.7. Growing centrality

One of the foundational principles of Bitcoin is its decentralised nature. The idea is that value is issued by collaborative mining where all the parties are validating transactions in the blockchain. Assuming that thousands of people are mining separately, the system remains decentralised and the prospect of a single entity gaining control of the network was seen as very remote. However, in June 2014 two computer scientists from Cornell University sounded the alarm [98], stating that a large mining conglomerate was becoming too powerful, and had actually reached 51 percent of all mining capacity for Bitcoin during a few hours. Essentially the system was no longer decentralised. Any entity controlling 51 percent of the mining power would accrue all of the Bitcoins mined while in majority. The controlling mining conglomerate could send false information to the blockchain, which would amount to altering transaction history [99].

As a result, the Bitcoin community panicked, with posts in forums and social media urging users of GHash.io, the mining conglomerate involved, to leave the pool to avoid it going over 51 percent again. Since the incident, Ghash.io made a statement declaring that they would take steps to avoid becoming too dominant again [100]. At the time of writing, Ghash.io use decreased to only two percent, but other large mining conglomerates have emerged with over 22 percent of total distribution [101].

Many Bitcoin enthusiasts have dismissed centralisation concerns, pointing out that the community polices itself adequately. They also note that miners migrated to other pools as soon as the 51 percent threshold was crossed [102]. More pragmatic developers have proposed technical solutions, such as implementing an algorithm that would force nodes to store the entire blockchain locally, which would help against a 51 percent conglomerate controlling the entire system [103].

The truth is that until a long-term technical solution is reached, Bitcoin's decentralised nature relies entirely on the good will of miners. If Bitcoin in its present shape reached an important share of the financial market, it would be possible for an entity with substantial computing power to take over the entire system. The prospect of a government or corporation taking over Bitcoin would be a real threat.

3.8. Computational inefficiency

A less-explored area of concern with Bitcoin is that, at least as currently implemented, it might be energy inefficient. Bitcoin generates value by requiring those who participate in the network to dedicate computing power to verify transactions. This presents two problems for the scalability of the network, namely the computational power required to mine BTC and the size of the blockchain itself.

The computational power dedicated to mining has continued to increase over time. In Bitcoin, computing power is called the hash rate, and the unit of measure is the hash/second, meaning a calculation per second. Ten tera hashes per second (Thash/s) means that the network is performing 10 trillion

calculations per second, with the hash rate at the time of writing standing at over 410 thousand Thash/s. Whichever way you measure it, that is an astounding amount of computing power used to produce value. O'Dwyer and Malone found that the entire Bitcoin network uses energy equal to that consumed in all of Ireland [104]. Even under normal circumstances, such a staggering amount of energy expenditure might prompt questions about Bitcoin's carbon footprint and other related environmental problems. Even if we ignore environmental issues, it is difficult to justify such consumption on economic grounds. O'Dwyer and Malone concluded in 2014 that "the cost of Bitcoin mining on commodity hardware now exceeds the value of the rewards". [105]

Another issue is that the size of the blockchain is starting to become a problem. At the time of writing it was reaching 40 gigabytes [106]. This has some practical implications for BTC as a currency, as the size of the blockchain may hinder the speed at which transactions are verified. Average transaction times vary a lot depending on network loads, but currently it ranges from 6–12 minutes per transaction [107]. As the blockchain size increases with more transactions, hosting of the entire blockchain could become a problem as well, as it is thought that the blockchain may reach three terabytes in size within 10 years [108].

4. Legal and regulatory issues

The decentralised nature of Bitcoin and a lack of a clear set of actors may prompt some to think that it is not possible or desirable to attempt to regulate the electronic currency. The fact that there is no issuing body and no central authority in charge of the payment scheme may lead one to believe that it is not even possible to undertake any sort of regulatory effort. However, Bitcoin has some practices that make some form of regulation necessary if it becomes widespread.

4.1. The legal nature of Bitcoin

In an episode of the popular TV series *The Good Wife*, appropriately entitled 'Bitcoin for dummies', a person who acts on behalf of 'Mr. Bitcoin', the anonymous and mysterious inventor of the cryptocurrency, hires the protagonist's law firm to defend him against a government action. The premise of the episode is that the U.S. Department of the Treasury wants to find the creator of Bitcoin because the digital currency is illegal in the United States. Although a crude depiction of the legalities of currency and commodities surrounding Bitcoin, the episode pinpoints some of the most pressing legal issues regarding their use. What is their legal status? Are they a currency? Are they a commodity? Are they a security? In short, is Bitcoin legal?

There are generally two types of currency from a legal perspective, legal tender and legal currency [109]. Legal tender is simply currency that cannot be refused in the fulfillment of a debt. Legal currency is money that is recognised by the government as a legitimate manner to pay for goods and services. In most countries legal currency and legal tender are one and the same, but there are some exceptions [110]. For example, there is something called a local currency, which is a currency that is usually accepted for payment in a local area, within a small number of participating stores [111]. Similarly, in the most of the U.K. the Bank of England notes are legal tender, but in Scotland and Northern Ireland, there are notes issued by several banks which act as legal currency. It is also common to see economies with a weak local currency accept international reserve currencies (for instance U.S. dollars or Euros) as legal currency [112].

4.1.1. United States regulatory response

In the United States, only the U.S. dollar is legal tender [113]. Similarly, only the Mint and the Federal Reserve can produce coins and currency, which are the only means of legal tender. Title 31 of the U.S. Code does not seem to make the distinction between legal currency and legal tender, so they appear to be treated in a similar fashion. This is corroborated by several official documents that indicate clearly that only the U.S. dollar is allowed as the official currency of the United States. According to the F.B.I. "it is a violation of federal law for individuals, [...] or organizations,[...] to create private coin or currency systems to compete with the official coinage and currency of the United States." [114] It would seem clear that local currencies that may compete with the dollar are not allowed, but the question of whether Bitcoin can be considered a currency for these purposes is not clear. There does not appear to be consensus that BTC would fall foul of regulation designed to protect the U.S. dollar as legal tender [115]. On the contrary, there have been electronic payment systems in existence for over a decade and there have not been attempts to curb them by using counterfeiting legislation [116].

However, all of the above does not mean that Bitcoin is illegal in the U.S. Because of many of the problems highlighted earlier, BTC is not currently used as a currency, perhaps with the exception of Web sites dealing in illegal goods in the 'dark Web' [117]. Bitcoin should be treated more like a speculative vehicle, more akin to securities or commodities, in which case its possible definition as a currency would not be necessary. Yang [118] makes a very strong case that Bitcoin can be considered a security under U.S. law, particularly because the definitions of a security present in the Securities Act of 1933 and the Securities Exchange Act of 1934 are broad enough to include all sort of bonds, debentures and certificates of interest as well as investment contracts. The very open definition was eventually used to classify as a security unusual investment contracts, such as citrus trees and earthworms [119]. The U.S. Supreme Court [120] has specifically defined an investment contract as an agreement that must involve "(1) an investment of money; (2) a common enterprise; and (3) an expectation of profits to derive solely from the efforts of others." [121] Yang argues that Bitcoin fulfills all of these three requirements, and therefore can easily be classified as a security, at least until

the law changes to classify it more adequately. It would also be easy for Bitcoin to be treated as a commodity under the broad definition present in the Commodity Exchange Act 1936, which offers a long list of goods that ends with the phrase "and all other goods and articles" [122].

4.1.2. European regulatory response

The situation in Europe and the U.K. is less ambiguous than in the U.S. First, there is considerably more regulatory acceptance for alternative currencies to those issued by central banks authorities, as evidenced by the aforementioned example of national legal currencies in the U.K., and a generally forgiving position for local currencies, such as the Bristol Pound, Brixton Pound and Lewes Pound [123]. These are very small payment schemes where a few participating retailers accept a note which acts more like a voucher and it is usually of very limited circulation. While BTC is larger by many degrees of magnitude, there does not seem to be any indication from regulators and central banking authorities in Europe that there will be a crackdown on Bitcoin over its legal status [124].

Second, Europe has already in place a legal framework for the regulation of electronic money, which could be used to cover virtual currencies such as Bitcoin. The Electronic Money Institutions Directive 2009/110/EC [125] contains rules for all sorts of electronic purses that can be used to store value in an electronic format, be it via a computer, a mobile device or online. The Directive defines electronic money thus (paraphrased for clarity):

1. electronically, including magnetically, stored monetary value;
2. as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions;
3. the transaction is an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;
4. which is accepted by a natural or legal person other than the electronic money issuer.

If a payment system fulfils these requirements, then it is considered electronic money, and only electronic money institutions (EMI) can issue electronic value. There is a high threshold for an electronic money institution, as the EMI would have to fulfil quite a number of requirements. The idea behind this stringent regulation is evident, as what is taking place is the issuing of value into the economy. Bitcoin would meet the legal definition to a certain extent, with the exception that it is not money that is issued in the sense that is meant by the Directive. As there is no central issuing authority, then it would be difficult to envision how financial services authorities in charge of regulating EMIs could intervene with regards to Bitcoin. If Bitcoins are not an EMI in Europe, then their status as currency is in doubt. The European Banking Authority (EBA) has opined that virtual currencies (VCs) do not fulfil many of the requirements of a currency, and therefore should not be considered legal tender:

> "VCs are not legal tender, which means the following features are not fulfilled: (a) mandatory acceptance, *i.e.*, that the creditor of a payment obligation cannot refuse currency unless the parties have agreed on other means of payment; (b) acceptance at full face value, *i.e.*, the monetary value is equal to the amount indicated; and (c) that the currency has the power to discharge debtors from their payment obligations." [126]

While it does not state directly, the EBA opinion infers Bitcoin being a commodity that can be exchanged for fiat money.

4.2. Regulatory actions to date

As some of the legalities surrounding Bitcoin are still not fully clear, there is still considerable scope for legislators and regulators to try to tackle the problems that might arise from the use of virtual currencies. Bitcoin users are learning the hard way why financial markets and currencies are heavily regulated areas. Deposit taking, the keeping of accounts, management of payment transactions, keeping of balances, all of these are functions of financial institutions that are of the utmost importance to businesses and consumers. The economy relies on financial intermediaries to operate and regulation is designed to prevent damage to consumers.

Regulators have been cautious in tackling some of the legal questions exposed by the emergence of cryptocurrencies. Part of the appeal of the payment system is that it is completely decentralised. Just as with P2P file sharing, you could shut down the entire Bitcoin intermediaries tomorrow and the network would still run because it does not depend on a central system. Bitcoin may very well be illegal, but almost impossible to shut down in any efficient manner, as a distributed network [127].

So what could regulators do? Based on Mayer-Schönberger and Crowley [128], we construct four scenarios for virtual currencies:

1. *'Virtual sovereigns':* virtual currency providers will serve as regulators by enforcing the terms of their contracts with users to prevent cyber-fraud and ensure proper behaviour.
2. *Prohibition:* governments could try to block their citizens from using virtual currencies that don't abide by government restrictions and regulations (governments have not been able to completely block access to Web sites nor will total prohibition on virtual currencies succeed).
3. *Selective prohibition:* government minimize the real-world impact of virtual currencies by, for instance, banning the sale of real-world goods for virtual currency. This section would also cover the banning and/or criminalisation of the use of the currency to pay for illegal activities or for money laundering.
4. *Selective regulation:* regulators impose some restrictions to specific aspects of virtual currencies, such as taxation and the regulation of intermediaries.

5. *'Real-world assisted virtual currency self-governance':* governments provide support for mechanisms whereby users of virtual currencies can agree upon and enforce their own 'community standards' and rules of conduct.

Note that 'do-nothing' option is a minor variant on Option 4 [129].

4.2.1. Virtual sovereigns

During the first few years of the existence of cryptocurrencies, the lack of any meaningful regulation or enforcement meant that intermediaries were left to self-regulate through terms of use and policies [130]. Interestingly, some commentators and participants in the economy advocate for either minimal regulation or to continue with the virtual sovereign approach [131]. The problem with this is that at the moment self-regulation has been translated into economic losses for unsuspecting users, as many exchanges and intermediaries were operating haphazardly or even fraudulently.

Lack of regulation of the sector has translated into a fertile ground for fraudsters and scam artists, from the existence of phishing sites passing off as exchanges [132], to online wallet services going bust. But the biggest example of the failure of self-regulation has to be the case of Mt. Gox. Mt. Gox was forced to file for bankruptcy in Japan after hackers allegedly managed to get into their system and steal US$446 million worth of bitcoins [133]. Some claim the site was riding a wave of speculation with coins that it did not have, accruing a large amount of debt. This is precisely the type of practice that regulation is supposed to stem.

4.2.2. Prohibition and selective prohibition

It should not be surprising that there has not been a regulatory push towards outright outlawing of Bitcoin, or any other cryptocurrency for that matter. There is no reason to suspect that governments feel threatened enough by Bitcoin at this time to warrant some form of ban, but most importantly, such an action could prove futile given the currency's decentralised nature [134].

Attempts at some partial prohibition of specific elements of the technology have been made. Thailand has attempted an outright ban on Bitcoin, although unsuccessfully. In 2013 a Thai company called Bitcoin Co. Ltd. was trying to register to operate in Thailand exchanging local currency for BTC, but the Foreign Exchange Administration and Policy Department declared that selling, buying, trading, exchanging and transferring bitcoins outside or within the country were illegal activities [135]. However, trading was re-opened six months later when the Bank of Thailand decided that the Foreign Exchange Administration lacked competence to ban BTC trading [136]. Russian regulators made some noise about cracking down on BTC trading but these never really materialised [137]. China has been the only jurisdiction to successfully attempt a major crackdown of Bitcoin. In December 2013, responding to claims of theft and fraud to Chinese nationals using BTC, the People's Bank of China made an announcement regarding Bitcoin in order to

"protect the public's property rights, to protect RMB's official currency status, to prevent money laundering risk and to protect financial stability." [138] The statement contains two very interesting measures. Firstly, it classifies BTC as a commodity and clearly disavows it as any type of currency. Then it seriously curbs its viability by restricting the way in which financial institutions may use it. The statement reads:

> "At this stage, all financial institutions and payment institutions must not use Bitcoin to set price for product or services, not buy or sell Bitcoins, not act as a market maker for Bitcoins, not underwrite insurance related to Bitcoin or cover Bitcoin in insurance, not directly or indirectly provide other Bitcoin related services, including registering, trading, clearing, settlement; not accept Bitcoin or use Bitcoin as payment tool; not start a Bitcoin and RMB or foreign currency exchange; not start a Bitcoin saving, trust or mortgage service; not issue Bitcoin related financial services; not use Bitcoin as the investment in trusts or funds."

While this is not a prohibition, it effectively restricted most of the currency-like functions of Bitcoin, as it could not be used to clear settlements or to make payments. The above meant that BTC operators could mostly trade it as a commodity, leaving out most other functions. It is curious that the announcement coincided with BTC's highest trading month and helped to push down prices considerably, heralding a crash that halved the price in less than a month [139].

It must be said that while the Chinese crackdown had some adverse effects on the use of Bitcoin as a currency [140], it is still being traded in China and the most active exchange is Chinese [141]. The yuan has overtaken the dollar as the top traded exchange currency in the Bitcoin economy [142]. The reason for this might be counterintuitive if we think of Bitcoin as a currency, but it makes sense if we see it as a commodity. BTC's popularity in China may be attributed to for domestic investors because, according to some analysts, "[t]here is not much else one can invest in." [143]

4.2.3. Selective regulation

Most of the regulatory responses so far have been related to taxation, and even these have been rather low key in comparison to the Chinese experiment [144]. In the United States, the Financial Crimes Enforcement Network (FinCEN) issued guidelines specified that decentralized currencies should comply with money laundering regulations [145]. In the U.K., Her Majesty's Revenue and Customs (HMRC) issued a briefing paper detailing its position on the tax treatment of income received from, and charges made in connection with, activities involving Bitcoin and other similar cryptocurrencies [146]. The HMRC recognises that this is an evolving regulatory area and is expecting that at some point there will be some sort of EU-wide effort to define and clarify cryptocurrencies in general. HMRC has in the interim decided to treat income from sales of goods and services through Bitcoin in the same manner as it does

any other sales. With regards to other income, they issued the following guidelines for the time being:

> 1. “Income received from Bitcoin mining activities will generally be outside the scope of VAT on the basis that the activity does not constitute an economic activity for VAT purposes because there is an insufficient link between any services provided and any consideration received.
>
> 2. Income received by miners for other activities, such as for the provision of services in connection with the verification of specific transactions for which specific charges are made, will be exempt from VAT under Article 135(1)(d) of the EU VAT Directive as falling within the definition of ‘transactions, including negotiation, concerning deposit and current accounts, payments, transfers, debts, cheques and other negotiable instruments.’
>
> 3. When Bitcoin is exchanged for Sterling or for foreign currencies, such as Euros or Dollars, no VAT will be due on the value of the Bitcoins themselves.
>
> 4. Charges (in whatever form) made over and above the value of the Bitcoin for arranging or carrying out any transactions in Bitcoin will be exempt from VAT under Article 135(1)(d) as outlined at 2 above.”

This brings it in line with other foreign currencies, and could be considered to be an official recognition of BTC’s status as yet another currency in the eyes of the law. However, as it has been mentioned repeatedly, Bitcoin is not behaving like a currency, continuing to behave mostly like a commodity.

This would bring it under the umbrella of securities and commodities regulators, such as the Security and Exchange Commission (SEC) or the Commodity Futures Trade Commission (CFTC) in the U.S. While these entities have not made any attempts to regulate Bitcoin directly, the SEC has imposed sanctions on unauthorised traders operating securities online for Bitcoin and Litecoin [147]. The SEC is also studying the approval of several securities companies operating as mutual fund and other Bitcoin-related financial instruments [148]. Finally, the SEC has issued a strongly worded statement warning investors interested in Bitcoin [149]. In it they point out some of the issues that we have enumerated earlier, such as the problem with the potential for losing bitcoins, lack of recourse if something goes wrong, and security concerns. They comment:

> “Both fraudsters and promoters of high-risk investment schemes may target Bitcoin users. The exchange rate of U.S. dollars to bitcoins has fluctuated dramatically since the first bitcoins were created. As the exchange rate of Bitcoin is significantly higher

> today, many early adopters of Bitcoin may have experienced an unexpected increase in wealth, making them attractive targets for fraudsters as well as promoters of high-risk investment opportunities."

European authorities seems to echo the warnings to consumers, with the European Banking Authority issuing a detailed list of potential risks for both consumers and investors that include many of those cited already, including monetary loss due to fraud, price instability, theft and the user's inexperience, which makes consumers unable to assess risk adequately [150].

4.2.5. Do nothing

The fact that there is little evidence of any growth in the use of BTC as a currency may be the reason why there have been minimal attempts to regulate it. The reason for this could be simply that the BTC market is just too small to warrant any wide-ranging regulatory effort. It is also possible that regulators simply do not understand the technology and its implications, awaiting any further developments to act.

Many regulators seem to be adopting the wait-and-see approach. Japanese authorities have stated [151] that they will monitor for illegal activity with Bitcoins, but will not regulate them for the time being. Similarly, Canadian regulators explain:

> "There could be potential risks to overall financial stability if Bitcoin became a significant means of payment and the Bitcoin system remained unstable [...] users need to be aware of the potential financial risks to which they might be exposed, in light of the ongoing volatility of bitcoin prices and the risk of failure of Bitcoin exchanges." [152]

However, there is concern that not taking any action will backfire on regulators. There are stories about illegal activities using Bitcoins, which eventually may prompt some form of action, at least to be seen as doing something to discourage blatant criminal activities. Similarly, news about fraud and exchanges becoming insolvent might also prompt some sort of action. Having provided a long list of risks for investors, users and financial institutions, the European Banking Authority issued the following warning to regulators against doing nothing:

> "Regulators themselves incur risks regardless of whether or not they do anything at all, deliberately decide not to regulate or decide to regulate but the approach fails. The risks may be of a legal nature, of a reputational nature or because the activity undermines one or more of the regulator's objectives. Unlike the risks in the previous categories, the mitigation of the risks listed below is firmly in the hands of the regulators." [153]

The argument from the European Banking Authority is that regulators could see their reputation diminished if they allow illegal or fraudulent activity to go unchecked, but they would also be facing legal action due to inactivity. The choice then is to take some form of regulation.

4.2.6. Specific regulation proposals

A few specific regulatory proposals of note have been drafted. The California legislature is considering a virtual currency bill [154], which mostly creates a requirement for registration to the relevant regulator body for any person or institution wishing to engage in any virtual currency business. The bill defines virtual currency as "any type of digital unit that is used as a medium of exchange or a form of digitally stored", but excludes units used in online games, or other digital units that "cannot be converted into, or redeemed for, fiat currency." This would tend to exclude vouchers, loyalty points and air miles. Bodies trading in digital currencies must obtain a licence to operate.

One of the most important regulatory developments in France was a 2014 report by the Minister of Finance, Michel Sapin [155]. While French authorities admit that Bitcoin does not pose a threat to financial markets, they have recognised that there is clearly room for concern with regards to criminal activity and fraud. These concerns are mostly about the anonymity of transactions, which could have tax and money laundering implications. Therefore, France has made clear regulatory direction with regards to virtual currencies. These are:

1. Limit anonymity by making it mandatory for intermediaries and exchanges to require proof of identity upon opening an account.
2. Clarify the taxation of virtual currencies with the publication of a set of instructions for consumers and regulators.
3. Propose a European-wide approach to Value Added Tax (VAT).
4. Propose, after discussion with industry, to cap payments in virtual currencies, similar to existing caps on cash payments.
5. Regulate at European level platforms that exchange virtual currencies against the official currency.

These measures are substantial and substantive, particularly with regards to anonymity and the requirement for identification. It will be interesting to see if such measures act as a deterrent against the creation of new intermediaries in France.

The European Banking Authority followed the lead of the French recommendations. In their aforementioned report on virtual currencies, they also listed a detailed number of possible regulatory responses to the challenges posed by virtual currencies [156]. Some of the main proposals include the following:

- *Creation of a scheme governance authority.* This will be a non-governmental entity that will be accountable to regulators and it will institution that will be a mandatory requirement for virtual currencies,

which will therefore operate as a financial institution. The authority will act as a central body that will have the responsibility of maintaining the public ledger and manage the currency's protocol(s).

- *Customer due diligence (CDD) requirements.* Exchanges and other consumer-facing intermediaries will have to collect identifying information.
- *Fitness and probity standards.* To diminish the chance of fraudulent activity, participating entities and individuals will have to pass probity standards present in other financial sector entities.
- *Mandatory incorporation.* Participating entities must be incorporated to ensure accountability and liability.
- *Transparent price formation and requirements against market abuse.* To avoid market manipulation and insider trading, intermediaries must comply with existing regulation against such practices in the financial sector.
- *Authorisation requirements.* Market participants must register to the relevant regulator and/or scheme governance authority, and must be authorised to operate.
- *A global regulatory approach.* Because of the international nature of VCs, there needs to be a coordinated international response by regulators around the world.
- *Evidence of secure IT systems.* Self-explanatory and required by independent audit.
- *Other standard procedures in financial institutions.* There are various proposals that are standard requirement for financial institutions. These include having a corporate governance scheme, operating with minimum required funds and separating client account currency from their own VCs.

Some of these proposals are nothing more than an attempt to bring VC institutions into the fold of the wider regulatory framework already in existence in the financial sector in general. Some of these could be easily adopted in the existing Bitcoin economy, such as requiring exchanges to register to authorities. Some will be more difficult to achieve and might very well destroy some of the unique features present in cryptocurrencies that make them so appealing to some in the first place. Needless to say, requiring the existence of a central body is anathema to the ethos of cryptocurrencies. Similarly, increased scrutiny comes at a price; these suggestions might increase transaction costs as well.

It is not possible at the moment to foresee what will happen next. If cryptocurrencies remain a niche interest by the technical elites, then it is difficult to foresee that any of the above recommendations will be implemented. If on the other hand Bitcoin and other VCs finally become widespread, then there will surely be some sort of regulation at some point.

5. Alternative uses of blockchain protocols

A blockchain is quite simply any open, cryptographic, decentralised ledger, so in theory it can be implemented into any sort of scheme, financial or not, that requires a record of transactions. As has been stated repeatedly, in Bitcoin the ledger is public and decentralised. Since anyone can check past, present and proposed transactions, there is increased reliability in the system. The main function of the blockchain in Bitcoin is to avoid the potential of double-spending money. However, the blockchain idea is independent of the existence of Bitcoin. In the off-line world, barring counterfeiting, it is impossible to double-spend money as people hold limited amounts of physical currency. Monetary transactions however more often occur as the digital movement of value from one account to the other [157]. The idea is for the holding institution to contain a master ledger, in other words a record of the money in all of the accounts, making it possible to follow movements from one to the other [158].

In order to have a viable blockchain alternative outside of the Bitcoin implementation, a developer can use existing protocols and open source code to create a verification mechanism that must fulfil three important functions key to any blockchain distribution. These are:

- *Proof of work.* The proof of work (POW) is the way in which Bitcoin rewards miners for conducting transaction verification operations, which are expensive computational transactions. Any blockchain alternative will have to have an alternative POW pay-out if the intention of the technology is not monetary. This could be social, such as solving mathematical equations or finding prime numbers [159].
- *Authentication.* This is the main function of a blockchain, the implementation must be designed to validate transactions securely and unequivocally [160].
- *Decentralization.* The blockchain must be decentralized, so copies of the entire ledger cannot be held centrally. This presents a few technical problems, such as the increasingly unmanageable size of the blockchain as more transactions accumulate [161].

There are hundreds of such potential applications in the financial markets, such as bonds, stocks and derivatives [162]; but it would also be possible to apply the same type of technology to automated contracts [163], or even copyright licensing agreements [164]. The idea is to attempt to bypass the difficulties of contract formation and other legal transactions by allocating rights and responsibilities through electronic tokens that then would be recorded in a common ledger. A recent report explains:

> "While all of the high-value applications of the first wave of blockchain innovation are explicitly financial, this is not the case for the second wave of blockchain innovation, which primarily rests on the idea of a 'smart contract.' Put simply, a smart contract uses software code to implement human intentions by dynamically carrying out instructions embedded in

> tokens associated with a contract, rather than relying on legal texts interpreted by courts, regulatory bodies or other legal institutions." [165]

But this would not only apply to contracts, but also to distributing and allocating rights within decentralised organizations themselves [166].

There are already a number of tools that are being developed to take advantage of the blockchain beyond payment systems and cryptocurrencies. One of the most publicised has been Project Ethereum [167] which creates "a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions." [168] In other words, Ethereum is a protocol for smart open ledgers where users can allocate their own rules and values. Ethereum has released an open source mining application to the public, directed mostly at developers, and users can mine its own currency called "ether" by allocating processing power to validate transactions. The system allows users to create legal documents that can be validated through the blockchain while at the same time allowing users to mine the new currency.

D-CENT (Decentralised Citizens ENgagement Technologies) is an European Union (http://dcentproject.eu/) project that has proposed the creation of a social blockchain toolset that will allow adopters to generate their own alternative currency. The interesting part of this scheme is that it changes the economically-minded proof of work with a social one, which will be decided upon by the community [169]. Another project called Chain [170] is proposing to use blockchain protocols to pay for mobile minutes, verify energy credits, store loyalty points and scrutinise securities. Many other projects are being announced routinely, with applications as varied as smart solar panels [171] and assistance to operate stock markets [172].

While these proposals are very interesting, IT law is replete with grandiose claims of life-changing technologies that will revolutionise lives. It is often too easy to fall prey to the latest meme adopted by some commentator [173]. Talk of the blockchain is reaching the level that previous technologies received, such as the cloud and 3D printing. While the reach of these is indeed great, we cannot lose sight of the limitations that exist within the Bitcoin environment. Furthermore, the idea of conducting legal transactions automatically by means of smart contracts and intelligent agents is not new [174]. Every generation brings a new crop of suggestions, claiming that we are about to make lawyers a thing of the past, with most transactions completed by computers, yet the legal profession persists [175].

Despite this critique of the Bitcoin meme hype, the blockchain itself has immense potential, particularly for transactions that require transparency, resilience and decentralisation.

6. Conclusions

This paper examined several areas related to cryptocurrencies. First, we outlined the basics of cryptocurrencies for a non-specialist audience. Second, we looked at the advantages presented by Bitcoin and examined problems with implementation. We then turned in depth to the practical and regulatory challenges presented by Bitcoin and crypto-currencies in general.

We conclude that though Bitcoin may be the equivalent of Second Life a decade later, a liberating technology that is overhyped and poorly executed, so blockchains may be the equivalent of Web 2.0 social networks, a truly transformative social technology. In the last year there has been a marked shift in the rhetoric emerging from the Bitcoin camp. While there are still (and probably will ever be) a core group of enthusiasts who believe in the cryptocurrency with a fervour matched only by the Free Software movement, Bitcoin has not matched the expectations of some proponents. Various crashes, and wave after wave of scandals and allegations of fraud have decidedly dented the perception that Bitcoin is the currency of the future. The relative difficulty in acquiring and spending BTC has meant that it has continued to elude mainstream acceptance. At the same, there are other electronic payment methods such as Apple Pay [176], launched in 2015. While Bitcoin may well recede from the public imagination in the future as a virtual currency, one aspect of the scheme is gaining momentum. It is the idea of a transparent, distributed and decentralised transaction ledger: the blockchain.

It is decreasingly accurate to call Bitcoin a currency. Money is a unit of account, store of value and medium of exchange. Bitcoin is none of those, in any serious sense. Bitcoin has too many problems to be the solution. An anonymous and decentralized payment system could indeed revolutionise the economy, help to end the disproportionate power of some banking systems and democratise monetary exchange. A system created by an anonymous cryptographer may not be the way of the future; true openness is needed for the next experiment to be successful.

The most interesting development arising from Bitcoin has nothing to do with the currency itself or with regulation. It is an idea that turns the blockchain, Bitcoin's proof-of-transaction open log, into a platform for creating a smart contract decentralised platform. We may very well be talking about blockchain in the future with Bitcoin as the first implementation of an open ledger.

Bitcoin is a revolutionary idea in achieving decentralisation, but the current implementation suffers from libertarian economic dogma and critical mistakes, such as the potential for a large entity with access to large computing power to control the public records. The blockchain could bring everything that is good about Bitcoin and translate it into decentralised applications. This will certainly merit further disinterested independent

research in the future, separated from the hype and financial self-interest of the Bitcoin community.

The wider research questions relate to the future of fiat currencies and the possibility of social production and sharing based on blockchains as the basis for the record of exchange [177]. Some proponents of blockchains and social production suggest it may supplant increasingly distrusted sovereign currencies [178]. Our research has been more limited to a critical exploration of the use of the first widely adopted non-proprietorial virtual currency, Bitcoin. We must remember that in the late nineteenth century that there was a fierce, agriculturally based mass resistance to fiat money, which failed. Overblown claims about blockchain enabled virtual currencies may similarly fall by the wayside with less mass mobilisation online or off-line. As a site of resistance to free market dogma, virtual currencies may be limited, but as an organising principle for cooperative sharing alongside the sovereign fiat currency capitalist market, it may have a stronger, if niche, future, just as cooperative movements gained coexistence with mass consumer capitalism in the previous 150 years. A new form of cooperative commons online may be enabled by blockchains, but it will most likely not be built on Bitcoins for the reasons we have identified in this paper.

About the authors

Andres Guadamuz is Senior Lecturer in Intellectual Property Law, School of Law, Politics and Sociology at the University of Sussex.
E-mail: a [dot] guadamuz [at] sussex [dot] ac [dot] uk

Chris Marsden is Professor of Media Law, School of Law, Politics and Sociology at the University of Sussex.
E-mail: c [dot] marsden [at] sussex [dot] ac [dot] uk

Acknowledgements

The first draft of this paper was case study prepared for Joint Research Area: Virtual Communities of the European Internet Science Consortium 7th Framework Programme, Network of Excellence, under Grant No. FP7–288021, in which network we collaborated with Dr. Jonathan Cave (Warwick), Dr. Alison Powell and Dr. Paolo Dini (LSE), Dr. Melanie de Rosnay (CNRS), Professor Juan Carlos de Martin (UNIBO) and others. Research was also funded by the European Commission JUST/2013/ACTION GRANTS Grant Agreement Number 4562 Openlaws, in which network we collaborated with Dr. Paolo Dini and colleagues at the London School of Economics, and others, on the application of virtual currencies to legal reputational markets. All errors and omissions remain our own.

Notes

1. See European Commission, 2010. "Digital agenda for Europe: Communication from the Commission" (26 August), at http://ec.europa.eu/digital-agenda/en/news/digital-agenda-europe-communication-commission-26082010.

2. Broadband infrastructure in rural areas was a focus of the American Recovery and Reinvestment Act of 2009. In Europe, for instance, industry 4.0, the Internet of things, intelligent transportation systems and smart cities are all initiatives using ICT-enabled innovations in respectively manufacturing, inventory control, distribution, urban planning and environment: see http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_en.htm.

3. P. Mason, 2015. "China's currency gambit and Labour's debate about quantitative easing: Old and new ways to cope with economic crisis," *Guardian* (16 August), at http://www.theguardian.com/commentisfree/2015/aug/16/china-labour-debate-currency-economic-crisis.

4. Icelandic krona have declined by almost 40 percent in value compared to £Sterling during 2008, and has maintained that 40 percent devaluation since: see http://www.xe.com/currencycharts/.

5. Robert Zoé, 2015. "Pirates largest party fourth month in row," *Iceland Review* (4 August), at http://icelandreview.com/news/2015/08/04/pirates-largest-party-fourth-month-row.

6. J. Bearman, 2015. "The untold story of Silk Road," *Wired*, at http://wrd.cm/1L6svlW.

7. J. Bartlett, 2014. *The dark net: Inside the digital underworld*. London: William Heinemann.

8. J. Mullin, 2015. "Sunk: How Ross Ulbricht ended up in prison for life," *Ars Technica* (29 May), at http://bit.ly/1M7ChnP.

9. Based on a search of 'Bitcoin' in the *Social Science Research Network* (http://papers.ssrn.com last accessed 19 August 2015). The original academic law review article was downloaded 11,140 times in four years until 19 August 2015: R. Grinberg, 2012. "Bitcoin: An innovative alternative digital currency," *Hastings Science & Technology Law Journal*, volume 4, number 1, pp. 159–207, at http://uchstlj.org/wp-content/uploads/2015/10/Bitcoin-An-Innovative-Alternative-Digital-Currency.pdf.

10. A. Guadamuz and C. Marsden, 2014. "Bitcoin: The wrong implementation of the right idea at the right time" (18 June), at http://ssrn.com/abstract=2526736 or http://dx.doi.org/10.2139/ssrn.2526736

— the 91st academic paper published on Bitcoin in SSRN since it rose to prominence.

11. For the beginner interested in cryptocurrency, see, for example, D. Forrester and M. Solomon, 2013. *Bitcoin explained: Today's complete guide to tomorrow's currency* (Charleston, S.C.: CreateSpace); A.M. Antonopoulos, 2015. *Mastering Bitcoin: Unlocking digital cryptocurrencies* (Sebastopol, Calif.: O'Reilly); D. Wilcox, 2014. *Bitcoin beginner's guide: Everything you need to know to become rich with Bitcoins* (Clydebank Publishing); C. Barski and C. Wilmer, 2014. *Bitcoin for the befuddled* (San Francisco: No Starch Press).

12. Amongst libertarian texts are B. Kelly, 2015. *The Bitcoin big bang: How alternative currencies are about to change the world* (Hoboken, N.J.: Wiley); P. Vigna and M.J. Casey, 2015. *The age of cryptocurrency: How Bitcoin and digital money are challenging the global economic order* (New York: St. Martin's Press).

13. N. Popper, 2014. *Digital gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money* (New York: Harper); D. Frisby, 2014. *Bitcoin: The future of money?* (London: Unbound); Y. Jenkins, 2015. Bitcoin: Millionaire maker or monopoly money? (Charleston, S.C.).

14. P. Anning, S. Hoegner and J. Brito, 2015. *The law of Bitcoin*. Bloomington, Ind.: iUniverse.

15. D.L.K. Cheun (editor), 2015. *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. Amsterdam : Elsevier/AP; P. Franco, 2015. *Understanding Bitcoin: Cryptography, engineering and economics*. Chichester, West Sussex: Wiley.

16. J. Robinson, 2014. *BitCon: The naked truth about Bitcoin*.

17. A useful introduction is M. Swan, 2015. *Blockchain: Blueprint for a new economy*. Sebastopol, Calif.: O'Reilly Media.

18. A. Guadamuz, "Virtual currency and virtual property revisited," *Technollama* (11 February 2013), at http://bit.ly/1MaeW4N. On regulation in virtual worlds see B.F. Fitzgerald, 1997. "Life in cyberspace: A simulating experience," *Computer and Telecommunications Law Review*, volume 3, number 3, pp. 136–138; R. Bond, 2009. "Business trends in virtual worlds and social networks — An overview of the legal and regulatory issues relating to intellectual property and money transactions," *Entertainment Law Review*, volume 20, number 4, pp. 121–128; S. James, 2008. "Social networking sites: Regulating the online 'Wild West' of Web 2.0," *Entertainment Law Review*, volume 19, number 2, pp. 17–50; K.L. Petrasic, 2013. "DATA's self-regulatory quest to legitimise virtual currencies," *E-Finance & Payments Law & Policy*, volume 7, number 9, pp. 6–7; M. Taylor and M. Matteucci, 2009 "Virtual worlds," *Computer and Telecommunications Law Review*, volume 15, number 5, pp. 124–147; B. Regnard-Weinrabe, M. Taylor and R. Savary,

2013. “Virtual currencies, the risks and the regulatory radar,” *E-Finance & Payments Law & Policy*, volume 7, number 7, pp. 10–11.

19. See reviews of earlier literature in J.M. Balkin and B. Noveck (editors), 2006. *The state of play: Law and virtual worlds*. New York University Press; T. Davies and B. Noveck (editors), 2006. *Online deliberation: Design, research, and practice*. CSLI Publications/University of Chicago Press; B. Noveck, 2006. “A democracy of groups,” *First Monday*, volume 10, number 11, at http://firstmonday.org/article/view/1289/1209.

20. The vast recent literature on Bitcoin and its legal challenges includes M.G. Munck, 2011. “Future payments in a disruptive digital world,” *E-Finance & Payments Law & Policy*, volume 5, number 4, pp. 12–13; A. Alleyne, 2010. “Virtual currencies: Can they classify as property?” *E-Finance & Payments Law & Policy*, volume 4, number 5, pp. 14–15; D. Tavan, 2013. “A brave new Bitcoin world?” *Banker* (August), pp. 74–76; M. Taylor, R. Savary, and B. Regnard-Weinrabe, 2013. “Virtual currencies,” *Computers & Law*, volume 24, number 3, pp. 31–34; T.A. Anderson, 2014. “Bitcoin — Is it just a fad? History, current status and future of the cyber-currency revolution,” *Journal of International Banking Law and Regulation*, volume 29, number 7, pp. 428–435; R. Courtneidge, 2014. “Crypto currencies and the regulators: Friends after all?” *E-Finance & Payments Law & Policy*, volume 8, number 2, pp. 8–9; J. Dixon, 2013. “The importance of an effective Bitcoin exchange market,” *E-Finance & Payments Law & Policy*, volume 7, number 6, pp. 6–7; E. Jankelewitz, D. Nemirovsky, B.I. Reyhani, and A. Vaziri, 2014. “Regulators respond to the big questions posed by Bitcoin,” *E-Finance & Payments Law & Policy*, volume 8, number 4, pp. 6–8; J. Meek, 2014. “Banks ‘killing’ bitcoin industry, expert warns,” *Operational Risk & Regulation*, volume 15, number 5, p. 10; J. Meek, 2014 “Funny money,” *Operational Risk & Regulation*, volume 15, number 2, pp. 23–25.

21. Take the successful FIFA series, where there is a thriving economy of card trading, where players purchase virtual cards of their favourite players. This can be done through virtual in-game currency which is earned by playing and winning games. But players can also use real money to obtain coins to boost their teams.

22. See the review by Second Life’s co-founder C. Ondrejka, 2004. “Aviators, moguls, fashionistas and barons: Economics and ownership in Second Life,” at http://ssrn.com/abstract=614663.

23. On gaming and virtual currencies see N.J. Gervassis, 2004. “In search of the value of online electronic personae: Commercial MMORPGs and the terms of participation in virtual communities,” *Journal of Information, Law & Technology*, volume 3; S. Anil, A.K.W. Jie, J.S.H. Min, and Q.C.W, Xiu, 2012. “Virtual property — A theoretical and empirical analysis,” *European Intellectual Property Review*, volume 34, number 3, pp. 188–202; R. Courtneidge and V. Lloyd, 2013. “Accepting Bitcoin as payment for online gambling services,” *World Online Gambling Law Report*, volume 12, number 2, 3–4; D. Margaritov, 2014. “Bitcoin: On the frontier of online gambling

innovation," *World Online Gambling Law Report*, volume 13, number 3, pp. 8–9.

24. On the role of social network gatekeepers, see K. Barzilai-Nahon, 2006. "Gatekeepers, virtual communities and the gated: Multidimensional tensions in cyberspace," *International Journal of Communications Law & Policy*, volume 11; D.B. Garrie and R. Wong, 2010. "Social networking: opening the floodgates to 'personal data'," *Computer and Telecommunications Law Review* volume 16, number 6, pp. 167–175; L.H. Gonzalez, 2013. "Habeo Facebook ergo sum? Issues around privacy and the right to be forgotten and the freedom of expression on online social networks," *Entertainment Law Review*, volume 24, number 3, pp. 83–87; T. Gray, T. Zeggane, and W. Maxwell, 2008. "US and EU authorities review privacy threats on social networking sites," *Entertainment Law Review*, volume 19, number 4, pp. 69–74; L. Hicks, 2010. "Through the privacy wall," *European Lawyer*, volume 98, p. 51.

25. The existence of these exchanges is one of the premises of N. Stephenson, 2011. *Reamde*. HarperCollins.

26. G. Davies and J.H. Bank 2002. *A history of money: From ancient times to the present day*. Third edition. Cardiff: University of Wales Press, p. 36.

27. Promissory notes developed, lost trust and were reintroduced at different periods in different societies with no exact date of introduction.

28. English King John's more infamous mistake than even signing Magna Carta was to lose his gold reserve and jewels in a flood in The Wash a week prior to his death.

29. Note that English 'pieces of eight' were an adaptation of 'peseta', a measure of silver in the Spanish Empire developed from its control over South American silver mines. In the Anglo-Saxon world, gold reserves discovered in Australia, South Africa, Yukon and California led to the long term adoption of the gold standard even in late capitalism, though this was reviled by populists, notably Presidential candidate William Jennings Bryan in his famous 'cross of gold' speech of 9 July 1896 calling for convertibility of gold to silver: http://historymatters.gmu.edu/d/5354/.

30. From the Latin "let it be done".

31. See D. Flint, 2014. "Computers and Internet: Are all modern currencies not virtual? — The Bitcoin phenomenon," *Business Law Review*, volume 35, number 2, pp. 60–62; R. Folsom and M. Cashman, 2014. "Digital currency: A primer," *Computers & Law*, volume 24, number 6, pp. 27–30.

32. S. Nakamoto, 2008. "Bitcoin: A peer-to-peer electronic cash system," at https://bitcoin.org/bitcoin.pdf.

33. "History of Bitcoin" (2015), http://historyofbitcoin.org/.

34. Bitcoin and the Silk Road became prominent with this article: A. Chen, "The underground Website where you can buy any drug imaginable," *Gawker* (1 June 2011), http://bit.ly/1My9klz.

35. See, for example, https://bitcointalk.org/.

36. S. Lui, 2013. "The demographics of Bitcoin," *Simulacrum*, at http://bit.ly/1FUXFru.

37. A. Yelowitz and M. Wilson, 2015. "Characteristics of Bitcoin users: An analysis of Google search data," *Applied Economics Letters*, volume 22, number 13, pp. 1,030–1,036.

38. G. Coleman, 2014. *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. London: Verso.

39. C. Soghoian, 2012. "Enforced community standards for research on users of the Tor anonymity network," Center for Applied Cybersecurity Research, Indiana University, also at *Financial cryptography and data security*, *Lecture Notes in Computer Science*, volume 7126, pp. 146–153.

40. This problem set of ideology and currency is discussed in depth in the EC FP7 grant agreement no. 610349 D-Cent project: http://dcentproject.eu/. See Denis Roio, Marco Sachy, Stefano Lucarelli, Bernard Lietaer and Francesca Bria, 2015. "D4.4 design of social digital currency" (31 March 2015), D-cent Project, at http://dcentproject.eu/wp-content/uploads/2015/05/D4.4-final_v4.pdf, describing the D-Cent Freecoin Toolchain.

41. This is not unlike gold, silver and diamond reserves, though new 'finds' in these commodities due to changing mining techniques and geopolitical conditions mean that greater liquidity can arise (*e.g.*, with entry of Warsaw Pact and many new sub-Saharan African nations into global trading system since 1990).

42. See https://en.bitcoin.it/wiki/Genesis_block.

43. See: L. Luu, R. Saha, I. Parameshwaran, P. Saxena and A. Hobor, 2015. "On power splitting games in distributed computation: The case of bitcoin pooled mining," *Cryptology ePrint Archive, Report* 2015/155, http://eprint.iacr.org; Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar and J.S. Rosenschein, 2015. "Bitcoin mining pools: A cooperative game theoretic analysis," *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, pp. 919–927.

44. T. Moore and N. Christin, 2013. "Beware the middleman: Empirical analysis of bitcoin-exchange risk," In: *Financial cryptography and data security*. Berlin: Springer, pp. 25–33.

45. R. Reynolds, "A bit too far?" *Terranova* (10 June 2011), at http://bit.ly/1mJtwFj. D. Ron and A. Shamir, 2012. "Quantitative analysis of

the full Bitcoin transaction graph," *Cryptology ePrint Archive, Report* 2012/584, at http://eprint.iacr.org/2012/584.

46. M. Vasek, M. Thornton, and T. Moore, 2014. "Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem," In: *Financial cryptography and data security*. Berlin: Springer, pp. 57–71.

47. Released under the MIT License, the code is found at https://github.com/bitcoin/bitcoin.

48. A. Hayes, 2015. "The decision to produce altcoins: Miners' arbitrage in cryptocurrency markets," *SSRN paper* 2579448, http://bit.ly/1MybbXF.

49. http://www.ixcoin.co/.

50. http://namecoin.info/.

51. https://litecoin.info/.

52. https://ripple.com/.

53. http://dogecoin.com/.

54. Market capitalization is obtained by multiplying the current value of a currency with the number of available coins.

55. http://knowyourmeme.com/memes/doge.

56. https://github.com/bitcoinxt/bitcoinxt.

57. http://coinmarketcap.com/currencies/bitcoin/. This figure may be an exaggeration, as many coins have been lost.

58. For comparison, the market capitalisation of Apple at the time of writing was US$741.16 billion, and that of Google was US$369.9 billion.

59. J. Bouoiyour, R. Selmi, and A. Tiwari, 2014. "Is Bitcoin business income or speculative bubble? Unconditional vs. conditional frequency domain analysis," *Research Papers in Economics (RePEc) working paper*, at http://bit.ly/1G3YHVq.

60. http://blockchain.info/.

61. "How does Bitcoin work" (2011), at https://bitcoin.org/en/how-it-works.

62. "Transaction fees explained" (2015), at https://en.bitcoin.it/wiki/Transaction_fees.

63. "Bitcoin transaction fees explained" (2014), http://bitcoinfees.com/.

64. R. Wu, 2014. "Why we accept Bitcoin," *Forbes* (12 February), at http://onforb.es/1JEHaao.

65. K. Kaskaloglu, 2014. "Near zero Bitcoin transaction fees Cannot last forever," *International Conference on Digital Security and Forensics (DigitalSec2014)*, at http://bit.ly/1SffTwJ.

66. N. Christin, 2013. "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace," *Proceedings of the 22nd International Conference on World Wide Web*, pp. 213–224.

67. E. Ploshay, 2013. "First Iranian Website open to Iranians to buy and sell Bitcoin," *Bitcoin Magazine* (18 July), at http://bit.ly/1QL2IRu.

68. S. Feld, M. Schönfeld and M. Werner, 2014. "Analyzing the deployment of Bitcoin's P2P Network under an AS-level perspective," *Procedia Computer Science*, volume 32, pp. 1,121–1,126.

69. J. Britto and A. Castillo, 2013. *Bitcoin: A primer for policymakers*. Arlington Va.: George Mason University, p. 14, at http://mercatus.org/publication/bitcoin-primer-policymakers.

70. J. Lukasiewicz, 2013. "Bitcoin 'market manipulators' strike on the weekend," *Coinsetter Blog* (3 June), at http://bit.ly/1MLy4XE.

71. J. Southurst, 2014. "A bot named Willy: Did Mt. Gox's automated trading pump Bitcoin's price?" *CoinDesk* (26 May), at http://bit.ly/1IJB1cH.

72. A. Madrigal, 2011. "Libertarian dream? A site where you buy drugs with digital dollars," *Atlantic* (1 June), at http://theatln.tc/1pvw0IK.

73. F. Reid and M. Harrigan, 2013. "An analysis of anonymity in the bitcoin system," In: Y. Altshuler, Y. Elovici, A.B. Cremers, N. Aharony and A. Pentland (editors). *Security and privacy in social networks*. New York: Springer, pp. 197–223; doi: http://dx.doi.org/10.1007/978-1-4614-4139-7_10. They used network analysis to trace transactions down a chain of distribution, and discovered that by treating transactions as a links in a network, and sender and recipients were vertices, they could get a very good idea of who was doing what. Moreover, they claim that this information can be easily cross-referenced with information in public spaces and intermediaries, so anonymity would be seriously compromised.

74. M. Netter, S. Herbst and G. Pernul, 2013. "Interdisciplinary impact analysis of privacy in social networks," In: Y. Altshuler, Y. Elovici, A.B. Cremers, N. Aharony and A. Pentland (editors). *Security and privacy in social networks*. New York: Springer, p. 13; doi: http://dx.doi.org/10.1007/978-1-4614-4139-7_2.

75. *Ibid.*, p. 22.

76. M. Ober, S. Katzenbeisser and K. Hamacher, 2013. ”Structure and anonymity of the bitcoin transaction graph,” *Future Internet*, volume 5, number 2, pp. 237–250.

77. *Ibid.*, p. 245.

78. M. Möser, 2013. “Anonymity of Bitcoin transactions,” *Münster Bitcoin Conference*, at http://bit.ly/1B8YJwb.

79. *Ibid.*, p. 9.

80. A. Guadamuz, 2015. “The Silk Road trial: Lessons for Internet regulation,” *Technollama* (15 June), at http://bit.ly/1KZEKQI.

81. One BTC was worth US$9.57 on 1 June 2011, and US$223.31 on 1 June 2015. For more historical data, see http://www.coindesk.com/price/.

82. N.T. Courtois, M. Grajek and R. Naik, 2013. “The unreasonable fundamental incertitudes behind Bitcoin mining, *arXiv*, at http://arxiv.org/abs/1310.7935.

83. M. Yglesias, 2013. “Bitcoin will spiral up and down forever,” *Slate* (10 April), at http://slate.me/1tZI4ni.

84. M. Ferdinando, 2014. “Hayek Money: The cryptocurrency price stability solution,” *SSRN Research Papers*, at http://ssrn.com/abstract=2425270.

85. Anecdotally, one of the authors lost 0.01 BTC when he mistakenly deleted the wallet file, the address is still there, it just cannot be accessed, see http://bit.ly/1G592gB.

86. D. Ron and A. Shamir, 2012. “Quantitative analysis of the full Bitcoin transaction graph,” *Cryptology ePrint Archive*, Report 2012/584, at http://eprint.iacr.org/2012/584. Note the “vigorous debate” over their methodology at http://bit.ly/1BbT0Gk.

87. J.W. Ratcliff, 2014. “Rise of the zombie Coins,” *LTB Blog* (22 June), at http://bit.ly/1BbSWGt.

88. If everyone kept their money and hid it under the mattress, then the economy would enter into a downward spiral, as businesses would have no revenue, so they could not employ people. See I. Fisher, 1933. “The debt-deflation theory of great depressions,” *Econometrica*, volume 1, number 4, pp. 337–357.

89. B.P. Hanley, 2013. “The false premises and promises of Bitcoin,” *arXiv*, at http://arxiv.org/abs/1312.2048.

90. D. Ron and A. Shamir, 2012. "Quantitative analysis of the full Bitcoin transaction graph," *Cryptology ePrint Archive*, Report 2012/584, at http://eprint.iacr.org/2012/584.

91. *Ibid.*

92. On criminal law issues in using Bitcoin, see D. Birch, 2007. "Money laundering in virtual worlds: Risk and reality," *E-Commerce Law & Policy*, volume 9, number 5, pp. 12–13; A.S.M. Irwin, J. Slay, K.–K.R. Choo and L. Lui, 2014. "Money laundering and terrorism financing in virtual environments: A feasibility study," *Journal of Money Laundering Control*, volume 17, number 1, pp. 50–75; doi: http://dx.doi.org/10.1108/JMLC-06-2013-0019; F. Mok and K. Tiah, 2014. "Singapore: money laundering — Virtual currencies," *Journal of International Banking Law & Regulation*, volume 29, number 7, p. N–69; S. Ramage, 2014. "Bit coins — Kiss of death to us all in the developed world," *Criminal Lawyers*, volume 220, pp. 1–2; M. Rees and R. Willis, 2014. "Virtual currencies — Virtual frauds?" *Fraud Intelligence*, pp. 17–19, at http://www.counter-fraud.com/fraud-types-n-z/online-fraud/virtual-currencies--virtual-frauds-96389.htm; E. Southall and M. Taylor, 2013. "Bitcoins," *Computer and Telecommunications Law Review*, volume 19, number 6, pp. 177–178; B. Stoeckert and T. O'Brien, 2014. "Impossible to ignore — Virtual currencies, the next challenge," *Money Laundering Bulletin*, volume 214, pp. 4–7; R. Stokes, 2012. "Virtual money laundering: The case of Bitcoin and the Linden dollar," *Information & Communications Technology Law*, volume 21, number 3, pp. 221–236;doi: http://dx.doi.org/10.1080/13600834.2012.744225; R.J. Straus, 2013. "The FinCEN virtual currency guidance: Neutering Bitcoin?" *E-Finance & Payments Law & Policy*, volume 7, number 4, p. 9; W. Stuber, 2014. "Brazil: virtual currencies — Pyramid financial schemes," *Journal of International Banking Law and Regulation*, volume 29, 7, pp. N–66–N–67; G. Varriale, 2013. "Bitcoin: Regulating the wild west," *International Financial Law Review* volume 30, number 28, p. 17.

93. See the famous xkcd comic about security failure at https://xkcd.com/538/.

94. See the famous 25k BTC theft from June 2011 at http://bit.ly/1BbV94N.

95. For a list of exchanges and individual heists, see http://bit.ly/1BbVggM.

96. M. Kiran and M. Stanett, 2015. "Bitcoin risk analysis," *NEMODE Policy Paper*, at http://bit.ly/1Kv0lnK.

97. In the U.K., see, for example, sections 83, 84 and 75 of the Consumer Credit Act 1974 (at http://www.legislation.gov.uk/ukpga/1974/39/contents), which provide consumers with wide-ranging protection for misuse of credit cards, and gives users recourse in case of breach of contract.

98. I. Eyal and E. Sirer, 2014. "It's time for a hard Bitcoin fork," *Hacking, Distributed* (13 June), at http://bit.ly/1nZezSx.

99. I. Eyal and E.G. Sirer, 2014. "Majority is not enough: Bitcoin mining is vulnerable," In: N. Christin and N. Safavi-Naini (editors). *Financial cryptography and data security*. *Lecture Notes in Computer Science*, volume 8437. Berlin: Springer, pp. 436–454; doi: http://dx.doi.org/10.1007/978-3-662-45472-5_28

100. See https://ghash.io/ghashio_press_release.pdf.

101. See https://blockchain.info/pools.

102. E. Faggart, 2014. "Bitcoin mining centralization: The market is fixing itself," *Coin Brief*, at http://bit.ly/1nZia3a.

103. See https://blog.ethereum.org/2014/06/19/mining/.

104. K.J. O'Dwyer and D. Malone, 2014. "Bitcoin mining and its energy footprint," p. 5, at https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf.

105. *Ibid.*, p. 4.

106. See https://blockchain.info/charts/blocks-size.

107. https://blockchain.info/charts/avg-confirmation-time.

108. A. Wagner, 2014. "Ensuring network scalibility: How to fight blockchain bloat," *Bitcoin Magazine* (6 November), at http://bit.ly/1SKI6Kb.

109. J.B. Konvisser, 1997. "Coins, notes, and bits: The case for legal tender on the Internet," *Harvard Journal of Law & Technology*, volume 10, number 2, pp. 321–352, at http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech321.pdf.

110. S. Lotz and G. Rocheteau, 2002. "On the launching of a new currency," *Journal of Money, Credit, and Banking*, volume 34, number 3, part 1, pp. 563–588; doi: http://dx.doi.org/10.1353/mcb.2002.0003.

111. L.D. Solomon, 1995. "Local currency: A legal and policy analysis," *Kansas Journal of Law & Public Policy*, volume 5, p. 59.

112. See http://www.acbi.org.uk/media/sni_notes_factsheet_nov12_copy1.pdf.

113. 31 U.S.C. § 5103, at https://www.gpo.gov/fdsys/granule/USCODE-2010-title31/USCODE-2010-title31-subtitleIV-chap51-subchapI-sec5103.

114. U.S. F.B.I., 2011. "Defendant convicted of minting his own currency" (18 February), at http://1.usa.gov/1Lan5ZT.

115. See D.A. Dion, 2013. "I'll gladly trade you two bits on Tuesday for a byte today: Bitcoin, regulating fraud in the e-conomy of hacker-cash,"

University of Illinois Journal of Law, Technology & Policy, volume 2013, pp. 165–201, at http://illinoisjltp.com/journal/wp-content/uploads/2013/05/Dion.pdf; and C.K. Elwell, M.M. Murphy and M.V. Seitzinger, 2015. Bitcoin: questions, answers, and analysis of legal issues. Congressional Research Service Paper, http://bit.ly/1HJXFQK. .

116. J.J. Doguet, 2012. "Nature of the form: Legal and regulatory issues surrounding the Bitcoin digital currency system," *Louisiana Law Review*, volume 73, number 4, pp. 1,119–1,153, at http://digitalcommons.law.lsu.edu/lalrev/vol73/iss4/9/.

117. J. Bartlett, 2014. *The dark net: Inside the digital underworld*. London: William Heinemann.

118. R. Yang, 2013. "When is Bitcoin a security under US securities law?" *Journal of Technology Law & Policy*, volume 18, number 2, p. 99.

119. *Ibid.*, p. 109.

120. In *SEC v. WJ. Howey Co.* 328 U.S. 293, 301 (1946); version at https://www.law.cornell.edu/supremecourt/text/328/293.

121. R. Yang, 2013. "When is Bitcoin a security under US securities law?" p. 109.

122. 7 U.S.C. §1a(9), at https://www.gpo.gov/fdsys/granule/USCODE-2011-title7/USCODE-2011-title7-chap1-sec1a.

123. M. Naqvi and J. Southgate, 2013. "Banknotes, local currencies and central bank objectives," *Bank of England Quarterly Bulletin*, pp. 317–325, at http://bit.ly/1Lb4OZu.

124. R. Ali, J. Barrdear, R. Clews and J. Southgate, 2014. "Innovations in payment technologies and the emergence of digital currencies," *Bank of England Quarterly Bulletin*, pp. 262–275, at http://bit.ly/1HK2k5d.

125. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

126. European Banking Authority (EBA), 2014. "EBA Opinion on 'virtual currencies'," EBA/Op/2014/08 (4 July), at http://bit.ly/1HOuUT5.

127. For more on the subject of regulation, see P. De Filippi, 2014. "Bitcoin: A regulatory nightmare to a libertarian dream," *Internet Policy Review*, volume 3, number 2, at http://bit.ly/1teQq8l; doi: http://dx.doi.org/10.14763/2014.2.286; and A. Mallard, C. Méadel and F. Musiani 2014. "The paradoxes of distributed trust: Peer-to-peer architecture and user confidence in Bitcoin," *Journal of Peer Production*, number 4, at

http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-paradoxes-of-distributed-trust/.

128. V. Mayer-Schönberger and J. Crowley, 2006. "Napster's Second Life? The regulatory challenges of virtual worlds," *Northwestern University Law Review*, volume 100, number 4, pp. 1,775–1,826. See also M. Gillen, 2007. "Managing virtual communities: Time to turn the whetstone?" *International Review of Law, Computers & Technology*, volume 21, number 3, pp. 211–220; doi: http://dx.doi.org/10.1080/13600860701701371.

129. See further C. Marsden, 2011. *Internet co-regulation:: European law, regulatory governance and legitimacy in cyberspace*. Cambridge: Cambridge University Press, at pp. 71–100 for virtual world regulation.

130. L.P. Nian and D.L.K. Chuen, 2015. "A light touch of regulation for virtual currencies," In: D.L.K. Chuen (editor). Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data. Amsterdam: Elsevier, pp. 309–326.

131. D. Sonderegger, 2015. "A regulatory and economic perplexity: Bitcoin needs just a bit of regulation," *Washington University Journal of Law & Policy*, volume 47, pp. 175–217, at http://openscholarship.wustl.edu/law_journal_law_policy/vol47/iss1/14/.

132. K. Dotson, 2011. "Mt. Gox warns Bitcoin popularity attracting increased phishing attacks," *Silicon Angle* (30 August), at http://bit.ly/1nZes9A.

133. "Proof of massive fraudulent trading activity at Mt. Gox, and how it has affected the price of Bitcoin," *Willy Report* (25 May 2014), at http://bit.ly/1nFIA82.

134. B. Weber, 2014. "Can Bitcoin compete with money?" *Journal of Peer Production*, number 4, at http://bit.ly/1gvL6Ng.

135. Bitcoin Co. Ltd., 2013. "Trading suspended due to Bank of Thailand advisement" (13 July), at http://bit.ly/1R3IZMV.

136. Bitcoin Co. Ltd., 2014. "Bitcoin trading re-opened" (31 January), at http://bit.ly/1J1aA2w.

137. A. Ostroukh, 2014. "Russia softens stance on Bitcoin: Central bank will allow use of virtual currency," *Wall Street Journal* (2 July), at http://on.wsj.com/1J1baNE.

138. People's Bank of China, 2013. "Notice on preventing Bitcoin risk" (5 December), at http://bit.ly/1J1cJLD; translation into English from this site, at http://bit.ly/1R3MjYz.

139. L.P. Nian and D.L.K. Chuen, 2015. "A light touch of regulation for virtual currencies," p. 315.

140. Particularly after it has stopped being used by electronic commerce outlets, see L.Y. Chen, 2014. "Bitcoin banned by Alibaba's Taobao after China tightens rules," *Bloomberg Business* (8 January), at http://bloom.bg/1J1fsVf.

141. http://bitcoincharts.com/markets/.

142. J.I. Wong, 2014. "China's market dominance poses questions about global Bitcoin trading flows," *CoinDesk* (27 September), at http://bit.ly/1R3Pqj9.

143. *Ibid.*

144. On Bitcoin, virtual currencies and taxation, see R. Asquith, 2014. "Bitcoin: Too big not to tax," *Accountancy*, volume 152, number 1447, p. 27; A. Atlas, 2014. "Bitcoin: Getting down to real business with virtual currency," *E-Commerce Law & Policy*, volume 16, number 4, pp. 5–6; A. Bal, 2013. "Stateless virtual money in the tax system," *European Taxation*, volume 53, number 7, pp. 351–356; M. Lambooij, 2014. "Retailers directly accepting Bitcoins: Tricky tax issues?" *Derivatives & Financial Instruments*, volume 16, number 3, pp. 138–144; H. Nemeczek and C. Schies, 2013. "German Ministry clarifies where Bitcoin falls under German law," *E-Finance & Payments Law & Policy*, volume 7, number 11, pp. 10–11; G. Nuttall, 2007 "Income earning in virtual worlds: Taxation issues," *E-Commerce Law & Policy*, volume 9, number 5, pp. 7–9.

145. U.S. Department of he Treasury. Financial Crimes Enforcement Network, 2013. "Application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies," FIN-2013-G001 (18 March), at http://1.usa.gov/1kWrsK7.

146. Her Majesty's Revenue and Customs, 2014. "Bitcoin and other similar cryptocurrencies," *Revenue and Customs Brief* 9, at http://bit.ly/1kWrBgE.

147. U.S. Securities Exchange Commission, 2014. "SEC sanctions operator of Bitcoin-related stock exchange for registration violations" (8 December), at http://1.usa.gov/1HOr4ti.

148. U.S. Securities Exchange Commission. Office of Investor Education and Advocacy, 2012. "Exchange-traded funds (ETFs)," *Investor Bulletin* (August), at http://1.usa.gov/1IiogAq.

149. US Securities Exchange Commission, 2014. "Investor alert: Bitcoin and other virtual currency-related investments" (7 May), at http://1.usa.gov/1HOtkRl.

150. European Banking Authority (EBA), 2014. "EBA Opinion on 'virtual currencies'," p. 25.

151. http://japandailypress.com/japan-to-monitor-illegal-bitcoin-activity-stops-short-of-regulation-1548441/.

152. http://www.bankofcanada.ca/wp-content/uploads/2014/05/boc-review-spring14-fung.pdf.

153. European Banking Authority (EBA), 2014. “EBA Opinion on ‘virtual currencies’,” p. 36.

154. California Legislature, 2015. “Virtual currency,” Assembly Bill 1326 (27 February), at http://bit.ly/1GbM9s4.

155. Ministére des Finances et des Comptes Publics, 2014. “Remise du rapport sur les monnaies virtuelles,” at http://bit.ly/1HOzG2V.

156. European Banking Authority (EBA), 2014. “EBA Opinion on ‘virtual currencies’,” pp. 39–43. For more about the proposal, see N. Vandezande, 2014. “Between Bitcoins and mobile payments: Will the European Commission’s new proposal provide more legal certainty?” *International Journal of Law and Information Technology*, volume 22, number 3, pp. 295–310; doi: http://dx.doi.org/10.1093/ijlit/eau003.

157. J. Britto and A. Castillo, 2013. *Bitcoin: A primer for policymakers*, p. 3.

158. R. Ali, J. Barrdear, R. Clews and J. Southgate, 2014. “Innovations in payment technologies and the emergence of digital currencies,” p. 267.

159. D. Roio, M. Scachy, S. Lucarelli, B. Lietaer and F. Bria, 2015. “Design of social digital currency,” FP7 — CAPS EU Project, http://bit.ly/1Ioz0wP, p. 16.

160. *Ibid.*, p. 17.

161. *Ibid.*, p. 18.

162. R. Ali, J. Barrdear, R. Clews and J. Southgate, 2014. “Innovations in payment technologies and the emergence of digital currencies,” p. 271.

163. A. Wright and P. de Filippi, 2015. “Decentralized blockchain technology and the rise of lex cryptographia,” at http://ssrn.com/abstract=2580664.

164. P. Van Valkenburgh, J. Dietz, P. de Filippi, H. Shadab, G. Xethalis and D. Bollier, 2015. “Distributed collaborative organisations: Distributed networks & regulatory frameworks,” at http://bit.ly/1LeE2PJ.

165. *Ibid.*, p. 7.

166. D. Bollier, 2015. “The blockchain: A promising new infrastructure for online commons,“ *David Bollier Blog* (4 March), at http://bit.ly/1LeDSIj.

167. https://www.ethereum.org/.

168. J.M. Leflet 2014. "A next-generation smart contract and decentralized application platform," at http://bit.ly/1TqTldO.

169. Bria, *et al.*, 2015. "Design of social digital currency", p. 28.

170. https://chain.com/.

171. http://bit.ly/1LeHUjR.

172. A. Hern, 2015. "Nasdaq bets on bitcoin's blockchain as the future of finance," *Guardian* (13 May), at http://gu.com/p/48pfp/stw.

173. The authors do not claim to be immune from this.

174. The inimitable Jon Bing was already writing about legal decision-making by automated systems in 1977, see J. Bing and T. Harvold, 1977. *Legal decisions and information systems*. *Publications of the Norwegian Research Center for Computers and Law*, number 5. Oslo: Universitetsforlaget.

175. P. Leith, 2010. "The rise and fall of the legal expert system," *European Journal of Law and Technology*, volume 1, number 1, at http://ejlt.org/article/view/14, reviews many such claims. Earlier, see R.E. Susskind, 1986. "Expert systems in law: A jurisprudential approach to artificial intelligence and legal reasoning," *Modern Law Review*, volume 49, number 2, pp. 168–194; doi: http://dx.doi.org/10.1111/j.1468-2230.1986.tb01683.x.

176. https://www.apple.com/apple-pay/.

177. P. Dini, 2012. "Community currencies and the quantification of social value in the digital economy," *London School of Economics and Political Science*, at http://eprints.lse.ac.uk/47349/.

178. Y. Benkler, 2011. *The penguin and the leviathan: How cooperation triumphs over self-interest*. New York: Crown Business.

Editorial history

Received 22 October 2015; accepted 7 December 2015.

A BIT OF A PROBLEM: NATIONAL AND EXTRATERRITORIAL REGULATION OF VIRTUAL CURRENCY IN THE AGE OF FINANCIAL DISINTERMEDIATION

Isaac Pflaum* and Emmeline Hateley†

Abstract

The recent development of virtual currencies, such as Bitcoin, as well as the computer networks that support them, have opened new avenues for the unbanked to reduce transaction costs and gain access to capital without reliance on existing remittance networks or traditional, often foreign, banking institutions that are the primary focus of Basel III. As this Paper will illustrate, however, the use of Bitcoin as a virtual currency is just the beginning of what can become a larger trend towards disintermediation of the delivery of financial services more generally. To realize the full potential of this revolutionary technology, however, it is essential that a coherent regulatory approach be developed that will address abuses of the technology, including fraud, money laundering, and tax evasion, such as what has recently been brought to light in the Silk Road case. In the absence of coordinated international action, a robust extraterritorial application of the U.S. Criminal Code appears to be the most viable option for the United States to shape the development of this technology as a legitimate complement to the international banking system. This Article begins with a discussion of what Bitcoin is, why it is important, and how it has been regulated to date in the United States and elsewhere. This is followed by a discussion, using the Silk Road case as a guide, of how the extraterritorial use of the U.S. Criminal

---

* Isaac Pflaum is a consultant at DisputeSoft, an expert witness firm specializing in liability issues arising in computer software cases. Mr. Pflaum is a licensed attorney and patent agent with extensive experience in IT and development of software for high-performance and parallel computing environments. Before joining DisputeSoft in 2013, he received an LL.M. and J.D. from Georgetown University Law Center. During law school, he interned with the White House Office of Science and Technology Policy, the U.S. Department of Justice, the U.S. International Trade Commission, the Court of Federal Claims and the U.S. Patent and Trademark Office. Prior to attending law school, Isaac received a master's degree in chemistry for developing massively parallel protein simulation software for the study of HIV and tuberculosis drug targets. Mr. Pflaum was also a guest researcher in the Computational Science Center at Brookhaven National Laboratory.

† Emmeline Hateley is a J.D. candidate at Georgetown University Law Center (2015); she received her B.S. in Business Administration (International Business), *cum laude*, at the University of Southern California.

Code provides a mechanism for regulating Bitcoin in the absence of a more coordinated international approach.

I. Introduction

The recent global economic crisis has prompted coordinated action regarding financial regulation by governments and central banking authorities, for example, in the form of the Basel III standards issued in December 2010 and subsequently updated in 2011 (Basel III).[1] Half of

1. Basel III was published in December 2010 and revised in June 2011. The text is available at http://www.bis.org/publ/bcbs189.htm. The Basel Committee on Banking Supervision (BCBS) is a committee of banking supervisory authorities, which was established by the central bank governors of the G-10 countries in 1975. More information regarding the BCBS and its membership is available at http://www.bis.org/bcbs/about.htm. Documents issued by the BCBS are available through the Bank for International Settlements Website at http://www.bis.org.

the world's population, however, remains "unbanked."[2] For the unbanked, reforms such as Basel III have little to offer, since these reforms do not address the fundamental issue that billions of individuals, including millions within the United States lack equitable access to banking services. Banking alternatives such as virtual currency that are secure and operate at low transaction cost may have the potential to fill this gap in the international banking landscape. However, this potential is unlikely to be fully realized unless these alternative financial services comply with the varied national regulatory regimes aimed at combating fraud, money laundering, and terrorism. Unfortunately, in contrast to the coordinated regulatory approach to reforming the international banking system exemplified by Basel III, international cooperation in the area of banking alternatives remains relatively aspirational. In particular, the international regulatory landscape for virtual currencies, such as Bitcoin, is a patchwork of inconsistent and incomplete attempts to counter criminal abuse of the technology that fails to recognize or prepare for the technology's transformative potential.[3]

II. Bitcoin Is More Than a "Virtual Currency"

"Virtual currency" is a medium of exchange circulated over a network, typically the Internet, that is not backed by a government[4]—an "electronic form of currency unbacked by any real asset and without specie, such as coin or precious metal."[5] Bitcoin was designed to reduce

2. *Finance & Development, June 2010—In Brief*, International Monetary Fund, http://www.imf.org/external/pubs/ft/fandd/2010/06/brief.htm.

3. On the lighter side, Bitcoin appears to have inspired an attempt to transform the musings of Ayn Rand into a reality; in 2013, a group of American Libertarians founded a self-sustaining organic farming community called Galt's Gulch Chile in central Chile with an economy based on Bitcoins. J.M.P., *Bitcoin Paradise*, The Economist (Dec. 25, 2013), http://www.economist.com/blogs/schumpeter/2013/12/libertarian-enclaves (registration required); *Galt's Gulch Chile Becomes First Libertarian Community Accepting Bitcoin*, Galt's Gulch Chile (Nov. 12, 2013), http://galtsgulchchile.com/News/Detail/10.

4. *Acting Assistant Attorney General Mythili Raman, Testimony Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 113th Cong. 1 (2013) (statement of Mythili Raman, Acting Assistant Attorney General).

5. Derek A. Dion, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash*, 2013 U. Ill. J.L. Tech & Pol'y 165, 167 (2013) ("Bitcoin is an example of a virtual currency, and, as such, it is not regulated by a central bank or any other form of governmental authority; instead, the supply of bitcoins is based on an algorithm which structures a decentralized peer-to-peer transaction system.").

transaction costs,[6] and it allows users to work together to validate transactions by creating a public record of the chain of custody of each bitcoin.[7] Bitcoin can be used to purchase items online, and some retail establishments have begun accepting bitcoin in exchange for gift cards or other purchases.[8] In a recent report, the Government Accountability Office (GAO) described Bitcoin as "a decentralized digital currency that uses a peer-to-peer computer network to move bitcoins around the world" and "a privately issued digital currency that exists only as a long string of numbers and letters in a user's computer file."[9] As the GAO report notes, the Bitcoin Network uses cryptography to prevent what is commonly referred to in Bitcoin circles as "double-spending."[10]

A. *The United States Has Defined Bitcoin as a Convertible Virtual Currency*

In the United States, the Treasury Department Financial Crimes Enforcement Network (FinCEN) issued regulations on March 18, 2013, addressing "convertible" virtual currency, such as Bitcoin, that "either has an equivalent value in real currency, or acts as a substitute for real currency."[11] The Department of Treasury regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance."[12] According to the Treasury, in contrast to real currency, "virtual" currency such as Bitcoin is a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency.[13] In particular, virtual currency does not have legal tender status in any jurisdiction.[14] Outside of the

---

6. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG (Mar. 24, 2009), https://Bitcoin.org/Bitcoin.pdf [hereinafter *Bitcoin White Paper*].

7. Sec. & Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2013 WL 4028182, at *1 (E.D. Tex. Aug. 6, 2013).

8. *Id.*

9. U.S. Gov't Accountability Office, GAO-13-506, Taxation of Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks, at p. 5 (2013) [hereinafter GAO Report].

10. *Id.*

11. DEPT. OF TREASURY. FINANCIAL APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES, FIN-2013-G001 (Mar. 18, 2013).

12. 31 C.F.R. § 1010.100(m).

13. DEPT. OF TREASURY, *supra* note 11.

14. *Id.*

United States, governments have begun to recognize the necessity of dealing with the issue of Bitcoin's characterization as well.[15]

B. *Bitcoin is a Distributed Record of Digital Signatures*

The Bitcoin technology was first described by one or more individuals in a paper published to the Internet under the pen name "Satoshi Nakamoto" in March 2009.[16] The Satoshi paper defines a bitcoin as "a chain of digital signatures"[17] recorded by a distributed time-stamp server in a cryptographically secured ledger called the "Block Chain."[18] Technologically, Bitcoin is nothing more than a combination of several commonplace technologies developed over the past ten years or so to support Internet commerce and peer-to-peer networking.[19] The principal components of Bitcoin are a distributed database that stores

---

15. For example, the Norwegian Tax Administration (NTA) has issued a "Principle Statement" providing that Bitcoins are a capital property, and not a currency. *Bruk av Bitcoins—skatte- og avgiftsmessige konsekvenser*, NTA (Nov. 11, 2013), http://translate.google.com/translate?hl=en&sl=no&u=http://www.skatteetaten.no/no/Radgiver/Rettskilder/Uttalelser/Prinsipputtalelser/Bruk-av-bitcoins--skatte--og-avgiftsmessige-konsekvenser/&prev=/search%3Fq%3DBruk%2Bav%2BBitcoins%2B%25E2%2580%2593%2Bskatte-%2Bog%2Bavgiftsmessige%2Bkonsekvenser%26espv%3D210%26es_sm%3D122 (last visited May 17, 2014). And on December 3, 2013, the central bank of China and four other central government ministries and commissions jointly issued the Notice on Precautions Against the Risks of Bitcoins, defining Bitcoin as a special "virtual commodity." The Notice said that by nature Bitcoin is not a currency and should not be circulated and used in the market as a currency. Banks and payment institutions in China are thus prohibited from dealing in Bitcoins. *China Bans Financial Companies From Bitcoin Transactions*, BLOOMBERG NEWS (Dec. 5, 2013), http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html; 关于防范比特币风险的通知 [Notice on Precautions Against the Risks of Bitcoins] (issued by the People's Bank of China, the Ministry of Industry and Information Technology, China Banking Regulatory Commission, China Securities Regulatory Commission, and China Insurance Regulatory Commission, Dec. 3, 2013) YIN FA, 2013, No. 289, http://www.pbc.gov.cn/publish/goutongjiaoliu/524/2013/20131205153156832222251/20131205153156832222251_.html (China). An unofficial English summary of the Notice is available at BTC CHINA, https://vip.btcchina.com/page/bocnotice2013 (last visited May 17, 2014). In contrast, according to German Authorities, Bitcoin are not legal tender, but rather units of value that function as a private means of payment or a substitute for currency in private multilateral transactions. Kreditwesengesetz [Banking Act] (updated Sept. 9, 1998), BUNDESGESETZBLATT I at 2776, as amended, http://www.gesetze-im-internet.de/kredwg/index.html (Ger.).

16. *See Bitcoin White Paper*, *supra* note 6.

17. *Id.* at 2. The most commonly used credential is a public key claimed by the owner, also referred to as that owner's Bitcoin address. The public key is a unique string of numbers and letters that is mathematically related to a second string of letters and numbers called a "private key." As the names imply, a private key provides security only if it is kept private, while a public key is shared with others to validate signatures produced using the private key.

18. *See Bitcoin White Paper*, *supra* note 6, at 1.

19. *See id.*

transaction records, the Block Chain, and a telecommunications network for broadcasting and validating those transactions, the "Bitcoin Network."[20]

C. *Bitcoin Ownership is Tracked through Transaction Records and Secured Through Cryptography*

The Bitcoin Network maintains the Block Chain as a shared ledger of all transactions conducted in bitcoin, including the parties to each transaction, the value of bitcoin transferred, and the conditions under which the transferee may "spend" the value of bitcoin they have received.[21] The Block Chain itself is merely a computer file maintained by many network participants, which is updated each time a new valid block of transactions is added to the Block Chain.[22] Transactions are broadcasted to network participants on a peer-to-peer basis globally over the Internet.[23] Certain participants, referred to as "Miners," receive these transactions, validate them against the ledger entries stored in the Block Chain, and attempt to incorporate valid transactions into blocks,[24] which are time-stamped using a cryptographic hash function subject to a "proof-of-work" requirement, discussed *infra* at notes 35-37 and accompanying text, and added to the Block Chain.[25] New blocks are broadcasted globally across the Network and saved by the many network participants in the United States and elsewhere, who each independently maintain copies of the Block Chain.[26] Each time a

20. *Id.*; *see* Nathaniel Popper, *Into the Bitcoin Mines*, N.Y. TIMES, Dec. 21, 2013 ("Today, all of the machines dedicated to mining Bitcoin have a computing power about 4,500 times the capacity of the United States government's mightiest supercomputer, the IBM Sequoia, according to calculations done by Michael B. Taylor, a professor at the University of California, San Diego. The computing capacity of the Bitcoin network has grown by around 30,000 percent since the beginning of the year.").

21. These conditions may include, for example, a date and time before which the Bitcoin cannot be spent, a required countersignature, and, most commonly, a requirement that only the intended recipient can spend the Bitcoin being sent.

22. *See Bitcoin White Paper*, *supra* note 6.

23. *Id.*

24. *Id.* Each Miner prepares a proposed new block to add to the Block Chain by first referring to the Block Chain to verify each transferors' ownership of the value of bitcoin being transferred in that block, and second by adding a special transaction record to the beginning of the block. *See also infra* note 40.

25. *See Bitcoin White Paper*, *supra* note 6, at 2-3.

26. Most network participants store the Block Chain in Random Access Memory (RAM) to ensure speedy retrieval of transaction records. Accordingly, as the Block Chain increases in size through the recordation of new transactions, greater computational resources would be required by each node (i.e., each participant on the Bitcoin Network) in order for that node to continue

new block of transactions is incorporated into the Block Chain, the Miner responsible receives a reward of newly created bitcoin and sometimes a commission.[27]

Ownership of bitcoin means the ability to transfer it to others.[28] The ability to transfer bitcoin is determined by the previous transferor's use of script signatures.[29] Typically, the script signature associated with a transaction will instruct the Bitcoin Network to verify the identity of the transferee against a value stored in the transaction itself.[30] The network will validate a subsequent transaction only if the transferee can provide a private key that corresponds to a value stored in the previous transaction record, wherein the new transferor may in turn include a new condition that must be met before the next owner can spend the bitcoin.[31]

Ownership of bitcoin further rests upon control over the wallet

---

caching the Block Chain in local memory. As of February 2014, caching the Block Chain locally required approximately 850 megabytes of memory. When a block is incorporated by over 50% of nodes on the network, it becomes part of the so-called "longest Block Chain" which is relied upon by Miners to validate future transactions. As such, the greater the number of nodes, the more secure the Bitcoin network becomes. In order to facilitate network participation by the greatest number of nodes, therefore, a de facto standard has arisen that minimizes the size of each new transaction record to only that information which is required to settle the transaction. In order to limit the size of new Blocks to a manageable level, the Block Chain contains "Merkle Tree" entries that provide a sort of "save point" that permits the chain of records to be validated without requiring every node to store every transaction ever conducted in the currency. In order for the network to function properly, however, some nodes must maintain public copies of the entire Block Chain (i.e., every transaction ever conducted using the "0" proof-of-work function). *See, e.g.*, https://blockchain.info/.

27. *See Transaction Commission*, BITCOIN WIKI, http://en.bitcoinwiki.org/Transaction_commission (last visited May 17, 2014) (discussing the mechanics of how commissions are calculated); *Controlled Supply*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Controlled_Currency_Supply (last visited May 17, 2014) (discussing how the number of Bitcoins rewarded to a successful miner is calculated and how this value changes over time).

28. *See Bitcoin White Paper*, *supra* note 6, at 2.

29. *Id.*

30. *Id.*

31. *See Transactions*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Transactions (last visited May 17, 2014). Indeed, without such a condition, any participant on the Bitcoin Network could spend the bitcoin being transferred. As such, most nodes on the Bitcoin Network will reject, and thus refuse to propagate, transaction requests that fail to include the required credentials from the record owner. Unlike with other platforms for delivering financial services, transactions conducted with bitcoin are irreversible by default. Methods, such as escrowing with a required countersignature, are supported by signature scripting and most nodes on the Network, but this feature is rarely used. As discussed below, fraud involving bitcoin theft is a significant risk for participants in the Bitcoin Network who do not utilize escrowing to require the signature of a trusted third party before transactions between untrusted parties are broadcasted to the Block Chain. On the

storing the private key or keys that may be used to spend the bitcoin assigned to the wallet owner's public Bitcoin address or addresses.[32] The verification instructions provided in the previous transaction may require more than one signature or some other condition to be satisfied, such as the passage of time, before the wallet owner's signature will affect a transfer.[33] However, in most cases, the private keys stored in an owner's wallet will be sufficient to consummate transactions.[34] As such, if the private keys stored in an owner's wallet are compromised, then the bitcoin associated with each of the addresses (public keys) tied to the wallet can be irreversibly transferred, i.e. stolen. To date, there is no mechanism for reversing Bitcoin transactions once they have been recorded in the Block Chain. Accordingly, ownership of bitcoin must be secured through the use of a strong wallet password or by physically securing the private keys, for example, by saving these keys to a storage media, destroying all other copies, and securing the media (and the private keys) in a safe.

Once a transaction has been created, a cryptographic hashing function is used to integrate the transaction record into the Block Chain.[35] Only one new block meeting a constraint, referred to as a "proof-of-work," will be added to the Block Chain.[36] The proof-of-work require-

---

flip-side, bitcoin payment services that employ escrowing may provide both a high level of security in the form of fraud prevention as well as potentially lower costs.

32. *See Bitcoin White Paper*, *supra* note 6, at 2. When a bitcoin transaction is broadcasted, the bitcoin a transferor attempts to spend from a given public key must correspond to bitcoin received by that public key in a previous transaction recorded in the Block Chain, as determined by the Miners reconciling the transaction records in the Block Chain corresponding to the public keys the transferor provides. A bitcoin wallet can contain multiple public-key-private-key pairs, where each public key has a corresponding private key that is used to sign transactions broadcasted from the wallet using that public key. A payee, or more typically a Miner, verifies these signatures by reference to the corresponding public key noted in the Block Chain in the previous transaction record to verify the chain of ownership, thus confirming that a sender is the record owner of the bitcoin being transferred.

33. *See Contracts*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Contracts (discussing the mechanics of using Bitcoin to execute complex transaction types).

34. By extension, although most wallets may be further secured by their owner using a password, as discussed below in the context of the Silk Road investigation, gaining access to a person's bitcoin wallet usually provides complete control over how that person's bitcoin is spent. With access to a wallet, for example, bitcoin can be irreversibly spent without including instructions for how it they may be re-spent—the digital equivalent of pouring a beer out on the side-walk.

35. *See Bitcoin White Paper*, *supra* note 6, at 2.

36. *See generally* Adam Back, HASHCASH—A DENIAL OF SERVICE COUNTER-MEASURE (2002), *available at* http://www.hashcash.org/papers/hashcash.pdf. The text of each proposed new block is hashed and the resulting string is tested against the constraint, referred to as the "proof-of-

ment, simply stated, is the requirement that each new hash must begin with a certain number of zeroes ("0"s) in order to be added to the Block Chain.[37] The number of zeroes required to meet the proof-of-work requirement is referred to as the "difficulty."[38] This simple mechanism provides a significant level of security that increases the further back in the Block Chain a transaction is recorded.[39]

D. *The Manner in Which Bitcoin Transactions Are Recorded May Result in Stratification of the Network*

While the Bitcoin Network can theoretically operate without transaction costs (i.e., commission-free), it is more likely that the Bitcoin Network will stratify into different speeds of recordation service. "Min-

work." For a proposed new block of transactions to be entered into the Block Chain, the text contained in the block must hash to a string beginning with a set number of zero, "0," values determined by the Bitcoin Network.

37. *Id.* The combination of hashing and the proof-of-work requirement provides that each block incorporated into the Block Chain requires significant computational resources to generate. Since each block in the Block Chain also contains the hash of the preceding block, the blocks comprising the Block Chain together contain a large amount of work that cannot be easily reproduced. For example, changing a block in the Block Chain requires the generation of a new block containing the hash of the preceding block. Thus, altering a record in the Block Chain requires regenerating all blocks that follow the altered block in the chain (i.e. redoing the work they demonstrate).

38. *See Bitcoin White Paper*, *supra* note 6, at 3. As the difficulty increases (i.e. more zeroes are required to incorporate new blocks in the Block Chain), more iterations are required on average to find a nonce that will produce a hash of a new proposed block meeting the proof-of-work requirement. The Bitcoin Network is designed to scale the difficulty automatically based upon the computational resources available to the Network as a whole, so that the rate at which new blocks are added to the Block Chain remains approximately constant at one new block each ten minutes. The distinction between the rate at which blocks are incorporated and the number of transactions included in new blocks is important to an understanding of how the Bitcoin Network moderates the rate at which blocks are added to the Block Chain as opposed to the size of the blocks added. If the use of the Bitcoin Network increases over time, then the number of transaction records included in each block, and thus the block size memory, will increase over time. As the number of Miners increases, the rate at which new blocks can be incorporated into the Block Chain increases, regardless of the block size, if the difficulty remains constant. As such, the Bitcoin Network is designed to change the difficulty automatically every two weeks based upon the moving average rate at which blocks were incorporated into the Block Chain during the previous two weeks. A moving average is essentially a weighted average that is weighed in favor of the most recent information. This feature of the protocol maintains the average execution time for a transaction at around 10 minutes and limits the rate at which new bitcoin can be created. The size of each new block entry, on the other hand, is limited only by the de facto standards regarding the contents of transaction records.

39. *See Bitcoin White Paper*, *supra* note 6, at 3.

ers" receive transactions posted to the Bitcoin Network in real time and form these transactions into "blocks."[40] Miners have complete discretion as to the transactions they choose to incorporate into the blocks they mine. Each time a proposed new block is prepared by a Miner, a special transaction record is added at the beginning of the block by the Miner.[41] The special transaction record transfers the sum of a reward and a commission to an address or addresses of the Miner's choosing. The reward is a set quantity of newly created Bitcoin that is determined by the Bitcoin protocol.[42] The commission is a variable quantity determined by the parties to each transaction.[43] Given that the reward for new blocks is fixed, as the average size of each new block swells due to growth in transaction volume, those paying the most commission will attract Miners who can afford to operate the greatest computational resources and thus have the best chance of reliably incorporating transactions into blocks quickly. Since the reward for entering a new block diminishes with increasing difficulty relative to the computational resources required to meet the proof-of-work requirement, transactions paying little or no commission have to rely upon Miners operating the computational resources with the lowest fixed costs.[44]

---

40. Registration Statement of the Winklevoss Bitcoin Trust, Amendment No. 2 to SEC Form S-1 Registration No. 333-189752 (Feb. 19, 2014), at 26. Each Miner prepares a proposed new block to add to the Block Chain by first referring to the Block Chain to verify each transferors' ownership of the value of bitcoin being transferred in that block, and second by adding a special transaction record to the beginning of the block.

41. *See* Registration Statement of the Winklevoss Bitcoin Trust, Amendment No. 2 to SEC Form S-1 Registration No. 333-189752 (Feb. 19, 2014), at 29; *id.* at 29.

42. *See, e.g., Protocol Rules*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Protocol_rules (last visited Apr. 28, 2014); *Bitcoin White Paper*, *supra* note 6, at 4. Currently, the Bitcoin Network permits Miners to assign a value of twenty-five newly created Bitcoin as a reward for successfully entering a new block into the Block Chain.

43. *See Bitcoin White Paper*, *supra* note 6, at 4. Miners may also claim a commission if the other transaction records entered into the block do not balance—for example, if one or more transferors have not entered "change" transactions to balance their previous transactions with those already stored in the new Block.

44. Currently, the greatest computational resources are available to Miners operating massively-parallel super-computers based upon chips specially designed to carry out the hashing algorithm used to verify transaction records and produce new blocks. The current model for low-cost Bitcoin mining is based upon distributed, collective mining carried out by thousands of individuals who coordinate their mining activity through a central server to form what is called a "mining pool." The server administering the mining pool divides the rewards and commissions generated by the creation of new blocks among the participants in the pool according to a pre-determined set of rules. *See* Registration Statement of the Winklevoss Bitcoin Trust, *supra* note 40, at 10, 29-30.

E. *The Bitcoin Network Can Support a Variety of Security Features and Layered Financial Services*

The existing Bitcoin protocol supports complex transaction types based upon certain conditions.[45] These conditions include escrow payments and refundable deposits requiring a countersignature, time-delayed transactions, and transactions conditioned upon a third party's answer to a question, such as "Is John Doe alive?"[46] It is also possible for other recordation and financial services to be layered over the virtual currency model of the Bitcoin Network.[47] For example, unspendable transactions can be used to record small text messages in the Block Chain.[48] Moreover, short blocks of text have been included within the script signature line within transaction records. As such, an identification number could also be included in a transaction recorded in the Block Chain.[49] This feature could be used to embed an International Securities Identification Number (ISIN)[50] or other identification number related to a physical or paper asset (e.g., a real currency, gold, or debt asset such as a credit card account number, mortgage, etc.), or a personal identification number, such as a tax ID within a transaction record. Thus, it has been proposed that the Bitcoin Network could be used to issue and trade securities, vote in shareholder elections, pay dividends, and support a host of complex financial products such as

---

45. *See, e.g.*, *Script*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Script (last visited Apr. 28, 2014).

46. *See Bitcoin White Paper*, *supra* note 6, at 1; https://en.bitcoin.it/wiki/Protocol_specification (accessed 4/22/2014); *Contracts*, BITCOIN WIKI, *supra* note 33.

47. *See* Hal Hodson, *Bitcon Moves Beyond Mere Money*, NEW SCIENTIST (Nov. 20, 2013); Stephan Tual, et al, *Etherium: A Next-Generation Smart Contract and Decentralized Application Platform* (4/19/2014) (available at: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper) (last accessed 4/22/2014); Nick Szabo, Formalizing and Securing Relationships on Public Networks, FIRST MONDAY (1997), *available at* http://firstmonday.org/ojs/index.php/fm/article/view/548/469.

48. *See, e.g.*, KEN SHIRRIFF'S BLOG (Feb. 16, 2014), http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html (last visited Apr. 22, 2014) (demonstrating various examples of embedded text in the Block Chain).

49. *See, e.g.*, *id.* (discussing several examples of text embedded in Bitcoin transaction records).

50. An International Securities Identification Number (ISIN) uniquely identifies a security. Its structure is defined in ISO 6166. Securities for which ISINs are issued include bonds, commercial paper, stocks and warrants. The ISIN code is a 12-character alpha-numerical code that does not contain information characterizing financial instruments but serves for uniform identification of a security at trading and settlement. *See Structure,* INTERNATIONAL SECURITIES IDENTIFICATION NUMBERS ORGANIZATION, http://www.isin.org/isin (last visited June 8, 2014).

derivatives, options, or swaps.[51] The Bitcoin protocol can be used to create specialty sub-networks for a variety of purposes.

Moreover, an organization seeking to build off of the Bitcoin Network can branch the Block Chain at any time by changing the proof-of-work requirement, for example, by requiring hashes of new Blocks on the branch to begin with "1"s instead of "0"s, so long as it has sufficient computational resources to maintain the branch. For example, a branch of the Bitcoin Network could be used to record interests in real property, store encrypted medical records, publish public notices, and register and exchange various interests in pooled assets such as securitized mortgage portfolios.[52] Most relevant to the foregoing discussion, a branch of the Block Chain operating under a new proof-of-work requirement can be used as a payments processing network for money transfer services, prepaid payment cards, and traditional credit-card-type services.[53]

F. *The Number of Bitcoin Units of Exchange is Orders of Magnitude Greater than the Nominal Supply of Bitcoins*

Although the Bitcoin Network has enormous potential, the slow growth of Bitcoin's market capitalization indicates that the virtual

---

51. *See, e.g.*, Bitcoin Wiki, *Smart Property*, https://en.bitcoin.it/wiki/Smart_Property (last visited Apr. 28, 2014); Jeremy Wagstaff, *Bitcoin's promise: a financial revolution the web's been waiting for*, THE SIDNEY MORNING NEWS, Mar. 23, 2014, *available at* http://www.smh.com.au/it-pro/business-it/bitcoins-promise-a-financial-revolution-the-webs-been-waiting-for-20140322-hvl1l.html; Nathan Schneider, *Code your own utopia: meet Ethereum, Bitcoins most ambitious successor*, AL JAZEERA AMERICA, Apr. 7, 2014, *available at* http://america.aljazeera.com/articles/2014/4/7/code-your-own-utopia meetethereumbitcoinasmostambitioussuccessor.html; Tim Swanson, *Chapter 8: Jack-of-All-Trades?*, GREAT CHAIN OF NUMBERS, Mar. 4, 2014, *available at* http://www.ofnumbers.com/2014/03/04/chapter-8-jack-of-all-trades/.

52. Adam Back, *Hashcrash-a denial of service counter-measure* (2002), http://www.hashcash.org/papers/hashcash.pdf. As with the Hashcrash system, the only constraint on the proof-of-work requirement is that it be recognized by a majority of participants. *See Bitcoin White Paper*, *supra* note 6, at 3-4. For users of a branch of the Block Chain, any proof of work requirement can be selected so long as it is accepted by a majority of the miners maintaining the branch. *See Alternative Chain*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Alternative_chain (last visited June 8, 2014) (discussing the use of alternative chains to support a variety of services in parallel with Bitcoin).

53. Although it is beyond the scope of this paper, it is worth noting that a branch of the Bitcoin network could be used to implement web 3.0 style user payments systems, for example, to compensate users of social media for the information they provide to websites. This technology could also be used to transact in encrypted information (e.g., medical records) and public information (e.g., campaign contributions). *See, e.g.*, *Alternative Chain, supra* note 52 (discussing the use of alternative chains to support a variety of services in parallel with Bitcoin).

currency may not have a meaningful impact for several years.[54] While the bitcoin protocol[55] provides that new bitcoins will continue to be created, the "production of bitcoins will slow according to a schedule until around 2140, when the last new fraction of bitcoin, known as a 'satoshi,' will be mined just shy of 21 million bitcoins."[56] Because the value of bitcoin floats with the market,[57] current data does not indicate the eventual volume of bitcoins that will exist in the economy in terms of U.S. dollars.[58] The current market capitalization of the bitcoin economy is estimated to be over $4 billion,[59] but in 2012 remittances from the United States and the European Union totaled nearly thirty-eight times that figure.[60]

As such, the supply of bitcoin would appear at first glance to be insufficient to support the growing remittances market. However, unlike real currency, bitcoin can be split into denominations down to the limit of numerical precision supported by the computers comprising the Bitcoin Network.[61] As such, the volume of bitcoin units of exchange currently in circulation is already greater than the sum of all the denominations of real currency currently in circulation globally. The 12.4 million bitcoin currently in circulation on the Bitcoin Network can theoretically support transactions denominated in units as small as 0.00000001, providing over 124 trillion units of exchange on a 32-bit network, more than enough to support all current and foreseeable uses of the Bitcoin Network.[62]

---

54. *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 113th Cong. (2013) (statement of Jerry Brito, Senior Research Fellow, Mercatus Center at George Mason University, p. 4).

55. *Protocol Rules*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Protocol_rules (last visited Apr. 28, 2014).

56. *See Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*, *supra* note 54.

57. *Id.*

58. *Id.*

59. *Id.*

60. *Bilateral Remittances Matrix 2012*, THE WORLD BANK http://econ.worldbank.org/ (last visited June 8, 2014) (follow "Research" hyperlink; then follow "Prospects" hyperlink; then follow "Migration and Remittances" hyperlink; then follow "Data" hyperlink); *See Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*, *supra* note 54.

61. *See What Do I Call the Various Denominations of Bitcoin*, BITCOIN WIKI, https://en.bitcoin.it/wiki/FAQ#What_do_I_call_the_various_denominations_of_bitcoin.3F (last visited June 8, 2014) (discussing the naming scheme applied to the various denominations of Bitcoin, including the "satoshi" which is smallest denomination currently possible. 0.000,000,01 BTC = 1 satoshi (pronounced sa-toh-shee).

62. *Id.* ("There are many arguments against the special case of 0.01 BTC since it is unlikely to represent anything meaningful as the Bitcoin economy grows (it certainly won't be the equivalent

III. Basel III, the Banking Gap, and the High Cost of Foreign Remittances

The Basel III standards[63] revise regulatory capital rules for banking organizations to impose more restrictive capital definitions, higher risk-weighted assets, additional capital buffers, and higher requirements for minimum capital ratios.[64] In addition to implementing some of these structural changes, the Basel III standards are partially implemented through final rules adopted by the Board of Governors of the Federal Reserve System in August 2012 and October 2013.[65] In the United States and other OECD countries, Basel III is intended to improve both the quality and quantity of capital held by banking organizations and to strengthen the international regulatory capital standards, in particular, to address the risks posed by systemically important financial institutions brought to light during the last global economic crisis.[66]

In addition to these developments, the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act) codifies the principle of the systemically important (i.e., "too big to fail")

---

of 0.01 USD, GBP or EUR). Equally, the inclusion of existing national currency denominations such as 'cent,' 'nickel,' 'dime,' 'pence,' 'pound,' 'kopek' and so on are to be discouraged."); A 64-bit network could theoretically support 100 billion, trillion units of account to a precision of 0.0000000000000001, using only the bitcoin currently in circulation.

63. Basel Committee on Banking Supervision, *Basel III: A global regulatory framework for more resilient banks and banking systems* (2011), http://www.bis.org/publ/bcbs189.pdf (Version of the Basel III capital rules reflecting the CVA modification); *See also* Basel Committee on Banking Supervision, *Basel III: The Liquidity Coverage Ratio and liquidity risk monitoring tools*, Bank of International Settlements (2013), http://www.bis.org/publ/bcbs238.pdf (summarizing the Basel III liquidity coverage ratio rules and liquidity monitoring framework issued by the Basel Committee).

64. Capital Rules: Regulatory Capital, Implementation of Basel III, Capital Adequacy, Transition Provisions, Prompt Corrective Action, Standardized Approach for Risk-weighted Assets, Market Discipline and Disclosure Requirements, Advanced Approaches Risk-Based Capital Rule, and Market Risk Capital Rule, 78 Fed. Reg. 198 (Oct. 11, 2013) (to be codified at 12 C.F.R. pts. 208, 217, & 225).

65. 12 C.F.R. pt. 234 (August 2, 2012) (final rule establishing risk-management standards for certain financial market utilities (FMUs) designated as systemically important by the Financial Stability Oversight Council); 78 F.R. pt. 60217-62291 (October 11, 2013) (final rule aligning the risk capital standards used by U.S. banking organizations with significant trading activities to calculate regulatory capital requirements for market risk with the Basel III revised capital framework).

66. *See* Basel Committee on Banking Supervision, *Basel III: The Liquidity Coverage Ratio and liquidity risk monitoring tools*, *supra* note 63.

financial institution.[67] It does so by permitting the Board of Governors of the Federal Reserve System to issue rules authorizing the Reserve to provide direct financial assistance to so-called Financial Market Utilities (FMUs)—banking organizations that are deemed systemically important by the Financial Stability Oversight Council.[68] This assistance may, for example, take the form of interest paid by the Federal Reserve on the balances maintained by or on behalf of FMUs that have insufficient funds or liquidity to make such payments.[69] This provision of the Dodd-Frank Act is demonstrative of the limitations of the Basel III reforms: despite efforts to address the risks posed by systemically important financial institutions, significant risks remain. The Dodd-Frank Act empowers the Federal Reserve to do what it could not do before: place the full faith and credit of the United States behind such institutions, without a specific authorization from Congress, if the risk management reforms issued under Basel III fail.

A. *Basel III and the Dodd-Frank Act May Help Protect Those in the Developing World Who Rely Upon Foreign Banks*

Taken together, Basel III and the Dodd-Frank Act have far-reaching consequences. Indeed, according to a recent International Monetary Fund (IMF) working paper, while on average 20% of banks in OECD countries are foreign, 50% of banking in non-OECD countries is conducted by banks that are organized and primarily regulated in a foreign jurisdiction.[70] According to the IMF working paper, in developing countries, foreign bank presence has been negatively related to

---

67. 12 U.S.C. § 5462(6).

68. Under section 803 of the Dodd-Frank Act, an FMU is defined as a person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person. Dodd-Frank § 803. is not codified as 12 U.S.C. § 5462. *See* 12 U.S.C. § 5462(6).

69. *Id.*

70. Stijn Claessens & Neeltje van Horen, *Foreign Banks: Trends, Impact and Financial Stability*, INTERNATIONAL MONETARY FUND (Working Paper, January 2012), http://www.imf.org/external/pubs/ft/wp/2012/wp1210.pdf; *But see* Thorsten Beck, Asli Demirguc-Kunt & Maria Soledad Martinez Peria, *Banking Services for Everyone? Barriers to Bank Access and Use around the World*, 22 THE WORLD BANK ECON. REVIEW 3, 397-430 (2008), https://openknowledge.worldbank.org/bitstream/handle/10986/4486/wber_22_3_397.pdf?sequence=1; Thorsten Beck et al., *Financing patterns around the world: Are small firms different?*, 89 J. FIN. ECON. 467, 467-87 (2008) (A 2007 World Bank Enterprise Surveys using global firm-level data, found that 87% of small and 93% of medium-sized enterprises in developing economies have access to a bank account. Even in Africa, the numbers are relatively high: 83% for small and 94% for medium-sized enterprises).

domestic credit creation.[71] Moreover, IMF data shows that during the recent global crisis, foreign banks reduced credit more than domestic banks, except when they dominated the host banking systems.[72] As such, for those in the developing world who rely upon foreign banks, as for those in OECD countries who are also directly exposed to the risks of the international banking system, the measures taken by the Federal Reserve and other central banking authorities in accordance with Basel III are a significant step towards avoiding a recurrence of the recent troubles.

B. *Money Orders Are the Most Popular Alternative Financial Service Purchased by the Millions of Unbanked Households in the United States*

While significant, Basel III does nothing to address issues faced by billions of individuals across the globe who do not utilize banking services. According to the IMF and World Bank, approximately half of the world's population is "unbanked."[73] Moreover, a significant percentage of individuals in the United States are unbanked or underbanked.[74] For example, a 2009 FDIC Household Survey determined that approximately 7.7% of U.S. households, or 9 million people, did not have a checking or a savings account.[75] The proportion of unbanked U.S. households identified by the survey, moreover, varied considerably among different racial and ethnic groups; an estimated 21.7% of African Americans, 19.3% of Hispanics, and 15.6% of American Indian/Alaskans did not have a savings, checking, money market, or brokerage account.[76]

Furthermore, the FDIC found that an additional 31.6% of African Americans, 28% of American Indian/Alaskans, and 24% of Hispanics relied upon money services businesses or certain other nonbank financial institutions for routine credit or remittance services.[77] In contrast, 96.5% of Asians and 96.7% of whites had a savings, checking, money market, or brokerage account and only 7.2% and 14.9%, respectively, relied upon non-bank financial institutions for basic financial ser-

71. *Id.*

72. *Id.*

73. *Finance & Development, June 2010—In Brief*, *supra* note 2.

74. *Id.*

75. FED. DEPOSIT INS. CORP., FDIC NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS 10 (2009), *available at* http://web.archive.org/web/20101204182351/http://www.fdic.gov/householdsurvey/Full_Report.pdf [hereinafter 2009 FDIC SURVEY].

76. *Id.* at 15.

77. *Id.* at 11.

vices.[78] A follow-up survey published in December 2012 found that the percentage of unbanked U.S. households increased during the recent recession from 7.7% in 2009 to 8.2% in 2012, a net increase of approximately 800,000 households.[79] Moreover, as in 2009, unbanked households were approximately split between those with no banking history and those with previous banking history, and approximately 40% of unbanked respondents stated that they were very unlikely to open a bank account in the near future.[80] In particular, the 2009 FDIC study found that nonbank money orders are, by far, the most popular alternative financial service purchased by unbanked households.[81] Bitcoin may offer these individuals a lower cost alternative to nonbank money orders, as well as other financial services traditionally provided by banks.

C. *Traditional Banking Services Remain Unavailable or Underutilized by Billions of the World's Poor, But Innovative Alternatives Are Gaining Traction*

In the international context, banking services remain unavailable or underutilized by billions of individuals. According to a recent survey of about 150,000 people in 148 countries by the World Bank, three quarters of the world's poor do not have a bank account.[82] In particular, the study, which forms part of the basis for the World Bank Global Financial Inclusion Database, or Global Findex, found that even among those in the developing world who do have a formal bank account, only 43% use their account to save and only 61% of account holders worldwide use their account to receive payments.[83] The report notes that the use of mobile phones to conduct money transfers, which allows

78. *Id.*

79. *See* FED. DEPOSIT INS. CORP., FDIC NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS, 4 (2012), *available at* http://www.fdic.gov/householdsurvey/.

80. *See id.* at 5.

81. *See* 2009 FDIC SURVEY, *supra* note 75, at 28-29 (54.0% of respondents used nonbank money orders; 38.2% used nonbank check cashing services; 14.3% used pawn shops; and 11.9% used RTO agreements. Unbanked households that use nonbank money orders tend to use them regularly. Over 80% of unbanked households that use nonbank money orders do so three or more times a year).

82. *See* World Bank, *Three Quarters of The World's Poor Are "Unbanked"* (Apr. 19, 2012), http://go.worldbank.org/72MAKHBAM0.

83. *Id.* In the press release announcing the study results, World Bank Group President Robert B. Zoellick was quoted as follows: "Providing financial services to the 2.5 billion people who are 'unbanked' could boost economic growth and opportunity for the world's poor . . . the power of financial services can really help people to pay for schooling, save for a home, or start a small

account holders to pay bills, make deposits, or conduct other transactions via text messaging, has expanded to 16% of the market in sub-Saharan Africa, where traditional banking has been hampered by transportation and other infrastructure problems.[84] For example, 68% of adults in Kenya use a mobile phone for money transactions.[85]

D. *Disintermediation of Cross-border Remittances Using Bitcoin Offers Several Potential Advantages Over Nonbank Financial Services*

Whatever advantages the use of methods such as text messaging to conduct financial transactions may be, such payment methods suffer from a lack of security and high transaction costs.[86] For the unbanked in the United States and across the globe, virtual currencies such as Bitcoin offer several advantages over commonly available nonbank financial services, including reduced transaction costs from removal of intermediary third parties.[87] Low transaction cost in combination with cryptographic security is particularly beneficial to persons in the United States and other OECD countries sending remittances to foreign jurisdictions where banking services are not commonly available or widely adopted. Cutting out the middleman in financial ser-

---

business that can provide jobs for others. This new report on the world's 'unbanked' makes the case: the more poor people are banking today, the more they are banking on their future." *Id.*

84. *Id.* In contrast to the racial divide between the banked and the unbanked in the United States, the World Bank study found that women make up a disproportionately large share of the unbanked internationally. For example, while 37% of women in developing countries have an account, 46% of men do. That gap is even bigger among those in poverty: women living below two dollars a day are 28% less likely than men to have a bank account. The study found that poverty is the principal barrier for many of the world's unbanked population, but fees as well as accessibility of branch locations are also significant impediments for many who might otherwise take advantage of banking services.

85. *Id.*

86. *See* Key Pousttchi & Martin Schurig, *Assessment of Today's Mobile Banking Applications from the View of Customer Requirements*, Proceedings of the Hawai'i International Conference on System Sciences, Jan. 5-8, 2004, at 6, *available at* http://mpra.ub.uni-muenchen.de/2913/ (SMS banking is not as secure as other conventional banking channels, like the ATM and internet banking); William Jack & Tavneet Suri, *Risk Sharing and Transactions Costs: Evidence from Kenya's Mobile Money Revolution*, 104 AM. ECON. REV. 183 (2014) (transaction costs are a limiting factor in the adoption of mobile money transfer services).

87. *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 113th Cong. (2013) (statement of Patrick Murck, General Counsel, the Bitcoin Foundation). Indeed, using the Internet as a tool for disintermediation (i.e., to remove intermediaries from the supply chain) is nothing new. Consider, for example, how the Internet has changed the ways in which travel is arranged or how consumer goods are purchased.

vices, however, is problematic, since the middleman is often the only regulated party to a transaction.

As noted above, there is potentially a large and quickly expanding market for Bitcoin and other virtual currencies if they become a viable substitute for more traditional methods of transferring funds and providing financial services across national borders.[88] According to a World Bank study published in October 2013, by year's end, the developing world was expected to receive $414 billion in remittances, a figure projected to increase to $540 billion by 2016.[89] Although these large numbers take into account outflows on a global basis, the outbound remittances from the United States and European Union members represent a significant portion of the global figure, with over $51 billion and $97 billion originating from these jurisdictions respectively.[90] Specifically regarding the United States, the largest volumes of remittances in 2012 went to Mexico ($22.8 billion), China ($13 billion), and India ($11 billion), but several Latin American nations, including Guatemala and El Salvador received high volumes ($4.4 billion and $3.6 billion respectively) relative to their populations, as well.[91]

E. *Bitcoin May Be Particularly Attractive to Those Remitting Funds Into States That Abuse Currency Controls*

In contrast to some Latin American nations such as Guatemala and El Salvador, Argentina and Venezuela (which have significantly larger populations but have enacted strict currency controls)[92] have received

---

88. Consider that in the area of financial services, Free Trade Agreements, such as the U.S.-Korea FTA, are intended to increase market access for cross-border suppliers of financial services. *See* Free Trade Agreement, U.S.-S. Kor., ch. 13 (June 30, 2007), http://www.ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text,

89. World Bank, *Migrants From Developing Countries to Send Home $414 billion in Earnings in 2013* (Oct. 2, 2013), http://www.worldbank.org/en/news/feature/2013/10/02/Migrants-from-developing-countries-to-send-home-414-billion-in-earnings-in-2013 ("The top recipients of officially recorded remittances for 2013 are India (with an estimated $71 billion), China ($60 billion), the Philippines ($26 billion), Mexico ($22 billion), Nigeria ($21 billion), and Egypt ($20 billion). Other large recipients include Pakistan, Bangladesh, Vietnam, and Ukraine.").

90. World Bank, *Bilateral Remittance Matrix 2012*, *available at* http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTDECPROSPECTS/0,,contentMDK:22759429pagePK:64165401piPK:64165026theSitePK:476883,00.html#Remittances.

91. *Id.*

92. *See, e.g.*, *Uncontained: Trade is the weakest link in the fight against dirty money*, THE ECONOMIST (May 3, 2014), http://www.economist.com/news/international/21601537-trade-weakest-link-fight-against-dirty-money-uncontained ("Organized crime funnels billions a year through the [Latin

relatively low volumes of remittances from the United States ($105 million and $44 million respectively).[93] A number of countries, including the United States, have similarly enacted exchange controls to combat terrorist financing and money laundering. Indeed, according to the IMF, between 2000 and 2005, the number of countries maintaining such restrictions increased from 69 (37% of reporting countries) to 104 (54.5% of total reporting countries).[94]

While counterterrorism efforts are a legitimate use of currency controls, Article VIII, Section 2(a) of the IMF Articles of Agreement denies recognition, subject to certain exceptions, of currency controls enacted by member states that impose "a direct governmental limitation on the availability or use of exchange as such."[95] Behind this prohibition lies the realization, as much through experience as theory, that when a nation abuses currency controls—for example, to restrict the making of payments relating to personal payments and trade—the result is often a shift to parallel currency markets.[96] Such a shift can create exchange disparities that distort economic decision-making and create opportunities for price arbitrage between types of transactions that would not exist in the absence of the currency controls.[97] While traditionally parallel currency markets have utilized foreign hard currency (e.g., U.S. dollars, euros, yen, etc.), persons seeking to circumvent currency controls in the twenty-first century have another option at their disposal: Bitcoin.

Bitcoin and other virtual currencies may provide a mechanism for individuals in countries with strict currency controls to circumvent exchange control measures, further increasing the potential global market for such currencies. Moreover, as a practical matter, currency controls that limit the ability of individuals within the countries to obtain foreign currency tend to favor those who engage in transactions

---

America's Black Market Peso Exchange], much of it to legitimate importers who cannot get enough dollars through official channels because of currency restrictions, for instance in Argentina and Venezuela. Some schemes combine formal and informal finance.").

93. *Id.*

94. *Article VIII Acceptance by IMF Members: Recent Trends and Implications for the Fund*, INTERNATIONAL MONETARY FUND (2006), https://www.imf.org/external/np/pp/eng/2006/052606.pdf.

95. *Selected Decisions and Selected Documents of the International Monetary Fund*, 36 Int'l Monetary Fund 590-92 (2011), https://www.imf.org/external/pubs/ft/sd/2012/123111.pdf (Decision No. 1034-(60/27), adopted June 1, 1960.).

96. PETER J. MONTIEL ET AL., INFORMAL MARKETS IN DEVELOPING COUNTRIES: A MACROECONOMIC ANALYSIS (1993).

97. *Id.*

that settle in foreign currency.[98] Accordingly, abuse of currency control measures encourages the use of Bitcoin in spite of the exchange and counterparty risks inherent in the use of an unregulated virtual currency.

F. *Bitcoin Provides an Alternative to the Black Market in Hard Currency for Persons Living in States that Abuse Currency Controls*

In practice, the consequences of Argentina and Venezuela's currency controls affect general currency inflows, outflows, and capital movement within these countries, and not just inbound remittances.[99] Argentina's and Venezuela's currency controls create investment barriers in both countries that discourage foreign parties from investing another form of currency in the nations' economies.[100] This barrier prevents more than just incremental remittances by individuals but also deters larger-scale foreign direct investment into the countries.[101] Furthermore, as noted above, from the point of view of the countries' citizens, the restrictions heighten the value of holding foreign currency—and virtual currencies such as Bitcoin—leading to black-market exchanges that boast more favorable, unofficial exchange rates, which may be partially responsible for inflationary pricing in these economies.[102] However, while Argentina and Venezuela's currency controls are among the strictest in the world today, they are by no means the only such restrictions. China's central bank requires that the settlement of currency exchanges be reported to and approved by the State Administration of Foreign Exchange.[103] It is no coincidence that

98. *See, e.g.*, Girish Gupta, *The 'Cheapest Country in the World'*, TIME (Jan. 23, 2014), *available at* http://world.time.com/2014/01/23/venezuelas-currency-controls-propels-those-with-connections/.

99. *See* Argentina Country Commercial Guide - Investment Climate, U.S. Dep't of Commerce Int'l Trade Admin., *available at* http://export.gov/argentina/doingbusinessinargentina/argentinacountrycommercialguide/investmentclimate/index.asp.

100. *Id.*

101. *Id.*

102. *See* Gupta, *supra* note 98; *see also* U.S. Dep't of Commerce Int'l Trade Admin., *supra* note 99.

103. *See, e.g.*, Notice of the General Affairs Department of the State Administration of Foreign Exchange on Relevant Issues concerning Opening Foreign Exchange Capital Accounts by Insurance Intermediary Institutions, Hui Zong Fa [2006] No.6 (Jan. 25, 2006) (English translation *available* at: http://english.mofcom.gov.cn/article/policyrelease/aaa/200606/20060602435969.shtml) (Giving notice of certain rules governing the role of the State Administration of Foreign Exchange in regulation of the branches and the administration departments of foreign exchange under the State Administration of Foreign Exchange the State Administration of

China's central bank was the first in the world to institute an outright ban on exchange between Bitcoin and the country's sovereign currency.[104] This precautionary measure was apparently intended to head off any potential threat that Bitcoin might pose to the capital controls imposed by the country's central bank.[105] Yet, despite the attempt of Chinese authorities to ban the exchange of sovereign currency for Bitcoin, the virtual currency is booming in China.[106]

G. *The Use of Bitcoin to Lower Transaction Costs on Foreign Remittances Furthers the Expressed Public Policy of the United States and Other OECD Countries*

Apart from providing an alternative to the black market in hard currency for persons living in countries with strict currency controls, Bitcoin's potential to lower transaction costs on foreign remittances furthers the expressed public policy of the United States and other OECD countries, particularly with regard to lowering the cost of sending funds to developing countries.[107] Indeed, transaction costs in

---

Foreign Exchange in all the provinces, autonomous regions, and municipalities directly under the Central Government, and the branches of the State Administration of Foreign Exchange in Shenzhen, Dalian, Qingdao, Xiamen and Ningbo).

104. *China Bans Financial Companies From Bitcoin Transactions*, BLOOMBERG NEWS, Dec. 5, 2013, *available at* http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html; 关于防范比特币风险的通知 [Notice on Precautions Against the Risks of Bitcoins] (issued by the People's Bank of China, the Ministry of Industry and Information Technology, China Banking Regulatory Commission, China Securities Regulatory Commission, and China Insurance Regulatory Commission, Dec. 3, 2013) YIN FA, 2013, No. 289, http://www.pbc.gov.cn/publish/goutongjiaoliu/524/2013/20131205153156832222251/20131205153156832222251_.html (China). An unofficial English summary of the Notice is available at BTC CHINA, https://vip.btcchina.com/page/bocnotice2013 (last visited Jan. 13, 2014). On December 3, 2013, China's central bank and four other central government ministries and commissions jointly issued the Notice on Precautions Against the Risks of Bitcoins. The Notice required that, at this stage, financial and payment institutions may not use Bitcoin pricing for products or services, buy or sell Bitcoins, or provide direct or indirect Bitcoin-related services to customers, including registering, trading, settling, clearing, or other services; accepting Bitcoins or using Bitcoins as a clearing tool; and trading Bitcoins with Chinese yuan or foreign currencies. *Id.*

105. China Bans Financial Companies From Bitcoin Transactions, BLOOMBERG NEWS, Dec. 5, 2013.

106. *See e.g.*, Pete Sweeney, *China gets first bitcoin ATM, skirting bank crackdown*, REUTERS, Apr. 16, 2014, *available at* http://www.reuters.com/article/2014/04/16/us-china-bitcoin-idUSBREA3F0MK20140416.

107. *Migration and Remittance Flows: Recent Trends and Outlook, 2013-2016*, THE WORLD BANK MIGRATION AND REMITTANCES TEAM, DEVELOPMENT PROSPECTS GROUP MIGRATION AND DEVELOPMENT BRIEF 21, 6 (Oct. 2, 2013), http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationandDevelopmentBrief21.pdf.

the foreign remittances market remain high. Despite "the G20 Objective of reducing costs to 5% in 5 years, the global average cost for sending remittances was 8.9% [to send $200], as measured by the World Bank's Remittance Prices Worldwide (RPW) database."[108]

Moreover, advances in technology have not yet resulted in a significant reduction in remittance fees.[109] While the global average remittance cost sits roughly around 9%, transaction fees vary widely based on the target region.[110] In addition to transmission fees for remittances, many banks have begun to charge "lifting" fees, which can be double the average sending cost for the recipient of the remittance.[111] These fees benefit the transfer services, such as Western Union, at a comparatively high cost to customers, often immigrants and poor individuals in developing countries. For example, according to its annual report for 2012, Western Union earned an operating profit of $1.3 billion from total revenue of $5.7 billion from 70 million senders at a rate of twenty-eight transactions per second.[112] Of the $5.7 billion revenue, Western Union "accumulated foreign earnings of approximately $4.4 billion as of December 31, 2012[.]"[113] Disintermediation of the remittances market through widespread adoption of Bitcoin could lower transaction costs to the point of making services such as Western Union obsolete, while at the same time helping to realize the G20 Objective of reducing costs to 5%.

H. *Bitcoin Offers an Alternative to the Remittance Services Offered by U.S. Banks, Which Are Primarily Limited Due to the Compliance Costs Involved in Dealing with Non-customers*

Remittances services offered by banks are limited, and Bitcoin has the potential to serve as a widely applicable alternative, albeit one that comes with its own set of risks. In particular, the response of banks to

108. *Id.*

109. *Id.* at 7 ("Remittance costs are falling in high-volume corridors . . . [evidenced by] the fact that the global weighted average remittance cost (weighted by the size of bilateral remittance flows) fell to 6.6 percent in the third quarter [of] 2013 . . . The persistence of high costs is inconsistent with the recent advances in technology and falling information costs.").

110. *Id.* For example, remittances to sub-Saharan Africa and East Asia/Pacific cost on average 12.1% and 9.0% respectively, while those to Latin America and the Caribbean cost 7.3%. *Id.*

111. *Id.*

112. WESTERN UNION, ANNUAL REPORT 2012, *ii*, http://ir.westernunion.com/English/investor-relations/financials/annual-reports/default.aspx (last visited Jan. 17, 2014).

113. *See id.* at 15.

compliance risks of dealing with non-customers may create incentives for those at the fringes of the traditional banking system to transition to bitcoin. For example, only 37% of U.S. banks surveyed by the FDIC in 2008 offered bank checks and money orders to non-customers, and only 6% of banks surveyed offered international remittance services to non-customers.[114]

Indeed, the FDIC Bank Survey found that "[p]roducts that are least often offered to non-customers are those that allow funds to be transferred internationally, specifically foreign currency exchange, international remittances, and automated clearinghouse (ACH) transfers," and that even when such products are available to non-customers, surveyed banks charged non-customers much higher fees than those charged to bank customers.[115] According to the FDIC survey, concerns related to customer identification, fraud, and compliance with the Patriot Act, Anti-Money Laundering Guidelines, and Bank Secrecy Act (BSA)[116] regulations were significant factors in the decision not to extend international remittance services to non-customers.[117] As discussed in detail in the following sections, however, the use of Bitcoin raises similar compliance concerns. As with Bitcoin's potential to undermine currency controls, however, rather than preventing the adoption of Bitcoin, the burden of regulatory compliance imposed by banks will likely contribute to the adoption of Bitcoin by those engaged in criminal activity. This is clearly problematic and threatens to undermine the potential Bitcoin has to transform the remittance services industry and benefit the billions of unbanked around the globe.

---

114. DOVE CONSULTING, BANKS' EFFORTS TO SERVE THE UNBANKED AND UNDERBANKED, FINAL REPORT FOR THE FEDERAL DEPOSIT INSURANCE CORPORATION, 10 (Dec. 2008) [hereinafter FDIC REPORT], *available at* http://fdic.gov/unbankedsurveys/2008survey/unbankedstudy/FDICBankSurvey_Report.pdf. (last visited May 24, 2014).

115. *Id.*

116. *See* 12 U.S.C. § 1818(s) (recordkeeping and recording requirements for federally insured depository institutions); 12 U.S.C. § 1786(q) (recordkeeping and recording requirements for federally insured credit unions).

117. FDIC REPORT, *supra* note 114., at 103 ("About three-quarters (196) of the banks state that obtaining sufficient identification information from non-customers to satisfy the Customer Identification Program (CIP), Know Your Customer (KYC), and Patriot Act regulations is a major challenge. The second most frequently mentioned topic of concern is compliance with the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML), which is reported by 83 banks.")

IV. Risks, Benefits, and Challenges Raised by the Disintermediation of Financial Services

A. *The Benefits of Bitcoin Must be Weighed Against the Risks Imposed by the Disintermediation of Financial Services*

As discussed in the preceding sections, the large volume of foreign remittances from the United States to developing countries and the relatively high cost of remitting money through traditional methods make the shift to Bitcoin particularly attractive. However, this is also attractive to those seeking to defraud Americans, fund terrorist activities, or remit the profits from the sale of illegal drugs. Bitcoin may offer the unbanked an alternative mechanism to transfer funds internationally, but by circumventing established intermediaries, Bitcoin exposes users to risks that regulatory regimes are intended to mitigate and impedes efforts of authorities and banks that are tasked with combating fraud, money laundering, and tax evasion.[118] Moreover, while both senders and receivers of Bitcoin payments may see Bitcoin as an economically efficient alternative to more traditional methods, such as wire transfers,[119] such users must bear risks posed by disintermediation, such as fraud, as well. Thus, for the potential benefits of disintermediation in financial services to be realized, regulatory authorities in the United States and elsewhere must address the risks posed by the regulatory gap that will be created by cutting out the middlemen.

B. *Anti-money Laundering Efforts Within the United States Illustrate the Difficulty of Developing an International Framework for Regulating Bitcoin*

Anti-money laundering (AML) efforts within the U.S. federal system provide some insight into likely hurdles to developing an international framework for regulating virtual currencies such as Bitcoin. Regulation of virtual currencies raises a difficult collective action problem. The need for cooperation and coordination between a plurality of federal

118. For example, the Bank Secrecy Act of 1970 (BSA), and the USA Patriot Act amendments to the BSA, require U.S. financial institutions to keep records of cash purchases of negotiable instruments of $3,000 or more and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. 31 U.S.C.A. §§ 5311-5330 (West), 12 USC §§ 1829b, 1951-1959 (West).

119. *See Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs, 113th Cong.* (2013) (statement of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network United States Department of the Treasury, p. 7).

and state entities is clear, but mechanisms for creating and maintaining the necessary collective knowledge remain illusive.

Treasury's efforts to ensure compliance with the Bank Secrecy Act (BSA) demonstrate how difficult it can be to enforce even relatively simple AML measures when sharing of information is required between multiple regulatory jurisdictions. The Treasury Department has substantial tools at its disposal to pursue its AML efforts.[120] Treasury's administration of the BSA through FinCEN, for example, is particularly relevant to a discussion of virtual currencies. In November 2012, the Treasury Department established a new AML task force composed of federal policymakers, regulators, and law enforcement agencies to examine and strengthen the U.S. AML framework.[121] Nonetheless, Treasury freely admits that neither FinCEN nor Treasury's Office of Foreign Assets Control (OFAC) presently have the resources or capability to maintain compliance with the current BSA regulatory framework without significant assistance from many partners at the state and federal levels.[122] Although FinCEN's efforts to promote cooperation between state and federal regulators are substantial,[123] there remain

---

120. *See* Letter from Inspector General Eric M. Thorson Memorandum to Secretary Geithner, Management and Performance Challenges Facing, OIG-CA-12-001 (Oct. 24, 2011). Treasury's Office of Terrorism and Financial Intelligence (TFI) is dedicated to disrupting the ability of terrorist organizations to fund their operations. TFI brings together intelligence gathering and analysis, economic sanctions, international cooperation, and private-sector cooperation to identify donors, financiers, and facilitators supporting terrorist organizations, and disrupt their ability to fund them.

121. According to the Department, "The Task Force's objective is to take a step-back look at our AML/CFT framework—from the legal and regulatory foundation, to the compliance and examination function, to the enforcement efforts—to take stock of which components of our regime are working well, which are not, how the different parts are working together, and to assess how the entire enterprise is operating." *Patterns of Abuse: Assessing Bank Secrecy Act Compliance and Enforcement: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs,* 113th Cong. 1 (Mar. 7, 2013) (Testimony of David S. Cohen, Undersec'y for Terrorism and Fin. Intelligence, U.S. Dep't of the Treasury).

122. *See* Treasury Fiscal Year 2013, TREAS. AGENCY FINANCIAL REP., at 155 (necessary partners include the four federal banking agencies, the IRS, the Securities and Exchange Commission, the Department of Justice as well as regulators in each of the fifty states. According to the Treasury Department, in Fiscal Year 2013, financial institutions filed approximately 18.7 million BSA reports, including nearly 1.8 million suspicious activity reports).

123. *See* Nathan J. Kutt, *FinCEN is Locked and Loaded—Does Your BSA Compliance Program have the Armor?*, COMPLIANCE DIGEST (Mar. 2014), http://www.wib.org/publications__resources/compliance_digest/mar_14/kutt.html ("FinCEN concerning potential fraud arising out of Bernie Madoff's investment scheme. Financial institutions should be aware that FinCEN has executed information sharing agreements—memorandums of understanding, or MoUs—with all Federal functional regulators, as well as with most states agencies (banking, insurance and gaming) in

significant gaps. For example, these commitments remain informal and non-binding and carry no penalties for violations.[124]

The significant efforts of Treasury to focus resources on strengthening and enhancing compliance with federal and state AML laws and regulations provides insight into how to cover the regulatory gap created by virtual currencies. In particular, it is not possible to regulate virtual currency effectively at the international level without significant assistance between states that permit its usage. Moreover, so long as commitments to international cooperation in this regard are informal, non-binding, and carry no penalties for violations, regulatory arbitrage will drive users of the currency towards operating in states with the lowest regulatory burdens. In a globally interconnected economy, it is essential to identify and plug the gaps in virtual currency regulation that encourage regulatory arbitrage and lowest common denominator regulation if the significant risks posed by criminal abuse of virtual currency are to be addressed.

Treasury's difficulties working with its partners at the state and federal level are hardly surprising. Indeed, the same coordination issues that have hampered Treasury's efforts are commonplace in international regulation.[125] More importantly, the difficulties experienced by Treasury indicate that coordinating at the international level may be very difficult, if not impossible. In particular, monitoring transactions within regulatory jurisdictions where virtual currencies become widely adopted could be exceedingly difficult due to disintermediation and inconsistent regulatory approaches. For example, in Canada, there has been no official rulemaking on the subject of

---

order to exchange supervisory information and receive raw data, i.e. examination results respecting deficiencies with an institution's BSA compliance program. And, in case you missed it, FinCEN in October 2013, executed an MOU with Mexico's National Banking and Securities Commission, most likely stemming from a $1.92 billion fine leveled against an overseas bank in December 2012 for arguably enabling Mexican drug cartels to launder cash through its branches.").

124. Letter from Inspector General Eric M. Thorson Memorandum to Secretary Geithner, Management and Performance Challenges Facing, OIG-CA-12-001 (October 24, 2011) ("While the number of SARs has been increasing since 2001, that alone does not necessarily indicate everything that is going well. [Treasury Department] audits have found problems with the quality of the data reported. Other audits have also identified gaps in the regulatory examination programs of the bank regulators and examining agencies.").

125. *See, e.g.*, U.S. DEP'T TREAS., FINANCIAL REGULATORY REFORM: A NEW FOUNDATION (2009); Steven Maijoor, Chair, Eur. Sec. & Mkts. Auth., International Coordination of the Regulation and Supervision of OTC Derivatives Markets, Proceedings of the 2013 American Bar Association Fall Conference (Oct. 17, 2013); HANS TIETMEYER, INTERNATIONAL COOPERATION AND COORDINATION IN THE AREA OF FINANCIAL MARKET SUPERVISION AND SURVEILLANCE (Feb. 11, 1999) *available at* https://www.financialstabilityboard.org/publications/r_9902.pdf.

Bitcoin, but the Financial Transactions and Reports Analysis Centre has reportedly sent out letters to a number of major Bitcoin service operators in Canada stating that they would not be subject to its rules or have to be registered with Canadian financial regulators.[126] Similarly, the German government has concluded that while licensing may become necessary in certain circumstances, such as market-making activity, no registration is necessary at this time to buy, sell, or exchange Bitcoin in Germany.[127] This aptly presents the collective action problem: if the Canadians and Germans are not collecting information about those engaged in Bitcoin transactions, these governments cannot share such information with U.S. authorities.

C. *The Approach Adopted in the United States Towards Regulating Bitcoin can be Significantly Improved*

In the United States, the U.S. Treasury has prioritized the sharing of information related to money services businesses (MSBs), including check cashers, currency dealers or exchangers, and money transmitters within the respective regulatory jurisdictions of state and federal authorities.[128] To address some of the issues specific to virtual currencies, in March 2013, FinCEN issued specific guidance on virtual currencies.[129] FinCEN's guidance classifies certain businesses and individuals that use convertible virtual currencies, or make a business of exchanging, accepting, and transmitting them, as MSBs.[130] Under the FinCEN guidance, persons "creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies" are subject to the MSB registration, reporting, and recordkeeping regulation.[131] However, the guidance also provides that "[a] user of virtual currency is not an MSB under FinCEN's regulations."[132]

FinCEN's rules governing Bitcoin are hardly comprehensive, but

---

126. Jasper Hamill, *Canadian Regulators Welcome US Bitcoin Refugees with Open Arms*, REGISTER (May 20, 2013), http://www.theregister.co.uk/2013/05/20/canada_welcomes_Bitcoin_traders_fintrac_letter/.

127. *Id.*

128. CONFERENCE OF STATE BANK SUPERVISORS, MEMORANDUM OF UNDERSTANDING BETWEEN THE INTERNAL REVENUE SERVICE AND [STATE REGULATORY AGENCY] CONCERNING MONEY SERVICES BUSINESSES AND CERTAIN OTHER NON-BANK FINANCIAL INSTITUTIONS, *available at* http://www.csbs.org/regulatory/Cooperative-Agreements/Documents/IRS-StatesBSA_MOU_4-22-2005.pdf.

129. FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 11.

130. *Id.*

131. *Id.*

132. *Id.*

Treasury's reliance on the existing AML framework within its regulations is an indication that regulatory authorities in the United States will apply available regulatory mechanisms, such as securities laws, to address concerns raised by the introduction of Bitcoin. For example, issuers of Bitcoin-backed securities would do well to remember that the securities laws apply to investment contracts that meet certain objective criteria, regardless of whether the asset in play is real or virtual.[133] Soliciting investments from investors creates security interests (whether or not backed by real or virtual currency), meaning that even investment vehicles employing Bitcoin are subject to Securities and Exchange Commission (SEC) enforcement under the Securities Act of 1933.[134]

The application of SEC regulation does provide some benefits to investors, however. For example, investors and issuers can protect themselves from uncertainty in the Bitcoin regulatory climate to some extent by bootstrapping the virtual currency into an existing regulatory niche, for example, by incorporating Bitcoins into an SEC-registered investment vehicle.[135] Moreover, if such issuers deal only with qualified investors, they will face a lower burden of disclosure and less potential liability under the securities laws, while meeting whatever market demand exists for Bitcoin-backed investments.[136] For example, the Winklevoss Bitcoin Trust, an exchange-traded fund currently pending approval by the SEC, has raised few public concerns from regulators, whereas in *S.E.C. v. Shavers* the unregistered issuance of Bitcoin-backed securities to unsophisticated investors was the subject of an SEC enforcement action.[137] The investment vehicles at issue in *S.E.C. v. Shavers* and the Winklevoss Bitcoin Trust registration fit nicely within the existing regulatory regime, but it is less clear how regulators will address other potential uses of Bitcoin, discussed above, such as the issuance of securities by persons in foreign jurisdictions.

---

133. S.E.C. v. Shavers, No. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013) (memorandum opinion holding that the court has subject matter jurisdiction).

134. *Shavers*, No. 4:13-CV-416 at 2. Shavers, a Texas resident, solicited local investors to buy and sell bitcoins as part of an interest-yielding investment scheme. In a civil proceeding brought against him by the SEC, Shavers argued that Bitcoin's absence from existing SEC regulations precluded his scheme from creating security interests in them. The court found that the exchangeability of Bitcoin for traditional currencies and the solicitation of individuals to give him money in a speculative fashion, however, meant that Shavers created an investment contract subject to the Securities Act of 1933.

135. *See* Winklevoss Bitcoin Trust, *supra* note 40.

136. *Id.*

137. *Compare* Winklevoss Bitcoin Trust, *supra* note 40, *with Shavers*, No. 4:13-CV-416.

In a similar fashion, by seeking to regulate MSBs dealing in Bitcoin, FinCEN has taken the first step towards reintroducing a regulated intermediary into Bitcoin transactions. FinCEN's distinction between MSBs and "users of Bitcoin," however, makes little sense and appears to demonstrate a lack of understanding of the protocol by which the Bitcoin Network operates. At bottom, "creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies" leaves little room for a distinct unregulated "user" of virtual currency.[138]

FinCEN, like the SEC, seems ill-equipped to deal with the disruptive potential of Bitcoin. For example, as noted above, the Bitcoin Network can support escrowing, refundable deposits, and conditional transactions (e.g., options, derivatives, and swaps). In the United States, these various financial products are regulated by a plurality of authorities at the state and federal levels.[139] Attempting to bootstrap each of these heads of the Bitcoin hydra into an existing regulatory framework would require that each responsible agency develop its own institutional knowledge while coping with disintermediation within the marketplace. As such, FinCEN's rules, as well as subsequent rules issued by other regulatory authorities, could be improved by focusing on those behaviors, such as exchanging, soliciting, and market-making, that bear reliable objective indicia that can provide more certainty regarding the regulatory status of Network participants.

---

138. FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 11.

139. *See* DEPARTMENT OF THE TREASURY, FINANCIAL REGULATORY REFORM: A NEW FOUNDATION 7 (2010), *available at* http://www.treasury.gov/initiatives/Documents/FinalReport_web.pdf (discussing the need for continuing reform within the context of overlapping and distinct responsibilities of the various federal and state agencies responsible for financial regulation in the United States) ("Prior to the current financial crisis, a number of federal and state regulations were in place to protect consumers against fraud and to promote understanding of financial products like credit cards and mortgages. But as abusive practices spread, particularly in the market for subprime and nontraditional mortgages, our regulatory framework proved inadequate in important ways. Multiple agencies have authority over consumer protection in financial products, but for historical reasons, the supervisory framework for enforcing those regulations had significant gaps and weaknesses. Banking regulators at the state and federal level had a potentially conflicting mission to promote safe and sound banking practices, while other agencies had a clear mission but limited tools and jurisdiction. Most critically in the run-up to the financial crisis, mortgage companies and other firms outside of the purview of bank regulation exploited that lack of clear accountability by selling mortgages and other products that were overly complicated and unsuited to borrowers' financial situation. Banks and thrifts followed suit, with disastrous results for consumers and the financial system").

D. *In Contrast to FinCEN's Efforts, the Regulatory Response Outside the United States Has Been Relatively Modest and Revenue-focused*

The European Union has not enacted any specific legislation related to the status of Bitcoin as a currency or otherwise, but momentum may be building behind an effort to converge European regulation of virtual currency.[140] In October 2012, however, the European Central Bank issued a report on virtual currency schemes that discusses the Bitcoin system and briefly analyzes its legal status under existing EU directives.[141] The report notes that the issue of Bitcoin regulation has been raised with the European Commission's Payments Committee.[142] The report also concludes, however, that neither the Electronic Money Directive 2009/110/EC, which permits EU authorities to regulate certain mediums of exchange that are stored electronically,[143] nor the Payment Services Directive 2007/64/EC,[144] which confers competency on the EU to regulate electronic payment services generally, provide the EU with the authority to regulate Bitcoin.[145]

States have made more progress in the area of taxing Bitcoin transactions. On March 3, 2013, the United Kingdom issued a Revenue & Customs Brief setting out the government's position on the tax treatment of income received from, and charges made in connection with, activities involving Bitcoin and other similar crypto currencies.[146] As the brief makes clear, however, the tax treatment of virtual currency

---

140. *See, e.g.*, Cecile Barbiere, *Paris Puts Bitcoin on EU Agenda*, EURACTIV.COM (Mar. 10, 2014), http://www.euractiv.com/euro-finance/paris-wants-put-bitcoin-eu-agend-news-534017 (reporting that the French Minister for Economy and Finance Pierre Moscovici would ask his European counterparts to take up the issue in a report submitted in April 2014) ("This is an imperative topic to be treated not only at national level but also at European level. In order to ensure this necessary convergence, I intend to request the other countries of the European Union to bring the topic on the agenda of the Ecofin Council").

141. EUROPEAN CENT. BANK, VIRTUAL CURRENCY SCHEMES (Oct. 2012), *available at* http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

142. *Id.* at 43.

143. Directive 2009/110, of the European Parliament and of the Council of 16 September 2009 on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions, Amending Directives 2005/60/EC and 2006/48/EC and Repealing Directive 2000/46/EC, 2009 O.J. (L 267) 7.

144. Directive 2007/64, of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market, Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and Repealing Directive 97/5/EC, 2007 O.J. (L 319) 1.

145. EUROPEAN CENT. BANK, *supra* note 141, at 43.

146. HM REVENUE AND CUSTOMS, REVENUE & CUSTOMS BRIEF 09/14, TAX TREATMENT OF ACTIVITIES INVOLVING BITCOIN AND OTHER SIMILAR CRYPTOCURRENCIES (2014), *available at* http://www.hmrc.gov.uk/briefs/vat/brief0914.htm.

in the United Kingdom in no way reflects how it will be treated for regulatory or other purposes.[147] Similarly, in April 2013, Canada's Revenue Agency reportedly stated that two separate tax rules apply to barter transactions and that certain types of speculation require users of Bitcoin to pay tax on transactions in the digital currency.[148] The German government, like the governments of the U.K. and Canada, has largely ignored Bitcoin except as a potential source of revenue.[149] The U.S. Treasury has followed this pattern, releasing guidance in 2014 making clear the government's position that Bitcoin transactions are taxable in the United States.[150] Despite the limited objectives served by these measures, as discussed in detail in the following sections, criminal prosecutions for tax evasion may be an effective mechanism for international financial regulation of Bitcoin.

V. Extraterritorial Application of the U.S. Criminal Code

In contrast to the patchwork of civil regulatory responses in the United States and elsewhere, the long arm of the U.S. Criminal Code appears to offer an effective and flexible set of tools to rein in the most egregious abuses of Bitcoin. To date, the most notable U.S. criminal enforcement activity involving Bitcoin is the Federal Bureau of Investigation's (FBI) seizure of Bitcoins used in connection with the underground website Silk Road.[151] On September 30, 2013, the FBI filed a

147. *Id.*

148. *Revenue Canada Says Bitcoins Aren't Tax Exempt*, CBC News (Apr. 26, 2013), http://www.cbc.ca/news/business/revenue-canada-says-Bitcoins-aren-t-tax-exempt-1.1395075.

149. Franz Nestler, *Deutschland erkennt Bitcoins als privates Geld an* [Germany Recognizes Bitcoins as Private Money], Frankfurter Allgemeine Zeitung (Aug. 16, 2013), http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-deutschland-erkennt-Bitcoins-als-privates-geld-an-12535059.html.

150. I.R.S. Notice 2014-21, 2014-16 I.R.B. 938. According to the IRS, wages paid to employees using virtual currency are taxable to the employee, must be reported by an employer, and are subject to federal income tax withholding and payroll taxes. Similarly, payments using virtual currency made to independent contractors and other service providers are taxable and self-employment tax rules generally apply.

151. *See* Press Release, FBI New York Field Office, Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of 'Silk Road' Website (Oct. 25, 2013), *available at* http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website. Silk Road functioned as a virtual black market that provided customers with an anonymous forum through which to receive bitcoins as payment for illegal activities such as the sale of narcotics. Hundreds of thousands of unique users from all over the world visited the site since its creation in 2011 to engage in illegal purchases of various products and services, such as computer

civil action in Manhattan Federal Court demanding the forfeiture of all of Silk Road's assets, including its Bitcoins, "because those assets were used to facilitate money laundering and constitute property involved in money laundering."[152] The FBI also filed an action individually against Ross William Ulbricht, also known as "Dread Pirate Roberts" or "DPR," on charges of narcotics conspiracy, conspiracy to commit computer hacking, and money laundering conspiracy for his alleged role as the owner and operator of the site.[153] This action led to the FBI's seizure of DPR's computer from his residence in San Francisco, including a personal Bitcoin wallet containing private keys corresponding to 173,991 Bitcoins with a market value of over $33.6 million dollars.[154]

A. *The Extraterritorial Reach of the U.S. Wire Fraud and Money-laundering Statutes is Extensive*

Foreign criminals using the Bitcoin Network may be prosecuted under the U.S. wire fraud,[155] money laundering,[156] aiding and abetting,[157] and conspiracy[158] statutes if they utilize the Bitcoin network for criminal activities. Despite the novel nature of using Bitcoins to commit financial crimes, such crimes nonetheless fall comfortably within the

---

hacking, forgeries, and drugs. In order to preserve the anonymity and decentralization of the marketplace's transactions, Silk Road only allowed payment by bitcoins through an "internal Bitcoin 'bank,' where every Silk Road user . . . had at least one Silk Road Bitcoin address associated with the user's Silk Road account." Silk Road managed the servers that maintained the Bitcoin wallets containing the addresses of the various users. A user interested in purchasing illegal goods or services through Silk Road obtained Bitcoins through a Bitcoin exchange and transferred these to an address associated with that user's Silk Road account. When a user made a purchase, Silk Road transferred the correct number of that user's Bitcoins to an escrow account until the transaction was completed, at which point the Bitcoins would move from the escrow account to the seller's Bitcoin address.

152. *Id.*

153. *Id.* DPR's alleged involvement in Silk Road was extensive, including oversight of every aspect of computer infrastructure maintenance and code programming, policy determination, staff management, and profit control. The FBI alleges that DPR possessed full knowledge of the illegal activities conducted on Silk Road, and that the decision to use Bitcoin as the exclusive currency for transactions facilitated by the website was intended to protect the anonymity of its users as well as DPR himself.

154. *Id.* This value is based on the Bitcoin exchange rate on October 25, 2013.

155. 18 U.S.C.A. § 1343 (West) (Technically, the wire fraud statute does not punish fraudulent schemes, only the illegal use of the U.S. telecommunications system in furtherance of such schemes).

156. 18 U.S.C.A. § 1956 (West).

157. 18 U.S.C.A. § 2(a) (West).

158. 18 U.S.C.A. § 371 (West).

jurisdictional provisions of these statutes by virtue of the fact that the Bitcoin Network makes extensive use of the U.S. telecommunications system to process and record transactions. Any criminal activity transacted in bitcoin necessarily occurs in part within the United States because the U.S. telecommunications system is used to process and record the related transactions.[159]

DPR is a U.S. citizen who is accused of committing criminal acts in the United States, and his Bitcoin wallet was located in the United States. To be sure, had DPR engaged in illegal activity abroad using the U.S. telecommunications infrastructure he would be subject to U.S. criminal jurisdiction under the wire fraud and money laundering statutes.[160] But even if DPR resided abroad and was a not a U.S. citizen, and the Silk Road site were hosted outside the United States, DPR would still have been subject to prosecution in the United States under several provisions of the U.S. Criminal Code that proscribe the use of U.S. telecommunications systems in connection with fraud that occurs *anywhere*.[161] The integral use of the Bitcoin Network and Block Chain in

---

159. *See* 18 U.S.C.A. § 1956(f) (West). There is extraterritorial jurisdiction for violations of § 1956 if: (1) the transaction or series of related transactions exceeds $10,000; and (2) the laundering is by a U.S. citizen, or, if by a foreign national, the conduct occurs in part in the United States; *But see* USAM 9-105.300, Approval Requirements for Money Laundering Cases ("Criminal Division (Asset Forfeiture & Money Laundering Section) (AFMLS) approval is required before the commencement of any investigation where jurisdiction to prosecute is based solely on the extraterritorial jurisdiction provisions of §§ 1956 and 1957. Due to the potential international sensitivities, as well as proof problems, involved in using these extraterritorial provisions, no grand jury investigation may be commenced, no indictment may be returned, and no complaint may be filed without the prior approval of AFMLS, Criminal Division when jurisdiction to prosecute these offenses exists only because of these extraterritorial provisions.").

160. The federal wire fraud statute outlaws schemes to defraud that involve the use of wire communications and may serve as a predicate offense for a charge of money laundering under 18 U.S.C. § 1956; 18 U.S.C. § 1343; *see also* Pasquantino et al. v. United States, 544 U.S. 349 (2005) (holding that a plot to defraud a foreign government of tax revenue violates the federal wire fraud statute because the plain terms of the statute criminalize such a scheme).

161. United States v. Kim, 246 F.3d 186, 190 (2d Cir. 2001) (Court of Appeals holding that the wire fraud statute could be extraterritorially applied to fraud against the United Nations by an American citizen on foreign soil that involved wire transmission to and from New York and that the defendant's knowledge that fraudulent invoices he approved were being paid by the United Nations through a New York bank was sufficient to allow the extraterritorial application of the wire fraud statute to his conduct while he was overseas, even though the actual wires were sent by innocent third parties; furthermore, holding that since the wire fraud statute could be applied extraterritorially to the defendant's conduct, jurisdiction also existed over the conspiracy counts arising from the same scheme); 18 U.S.C.A. § 1956(f) (West); Criminal indictment filed in *United States v Banco de Occidente*, S.A, in Mar. 1989. Cited in Matthew S. Morgan, "Money Laundering: The United States Law and Its Global Influence," Essay in International Financial

the commission of the same or similar crimes is sufficient to provide jurisdiction over a non-citizen acting outside the United States.

For example, U.S. authorities have prosecuted individuals for tax evasion that occurred in a foreign jurisdiction under the U.S. wire fraud statute based solely upon the use of the U.S. telecommunications network.[162] Similarly, in a prosecution under the money laundering statute, U.S. prosecutors defeated a jurisdictional challenge to the freezing of a Colombian bank's assets in West Germany, Canada, and Switzerland, despite the fact that the bank had no ties whatsoever to the United States.[163] The court justified its jurisdiction on the basis that the frozen funds represented substitute funds from drug proceeds that had been funneled from the United States to the bank's branch in Colombia through an intermediary in Panama.[164] In other words, the court refused to dismiss the indictment on the basis that part of the alleged criminal conduct giving rise to the funds held by the bank in Colombia occurred in the United States.[165] Similarly, users of the Silk Road site took advantage of the Bitcoin Network, and used the telecommunications system of the United States in the process, to evade taxes in

---

and Economic Law No.5, 1996 ("Banco De Occidente was a Columbian bank with absolutely no connection to or presence in the U.S. The U.S. government alleged that Panamanian branch of Banco de Occidente have received transfers of drug money from another bank located within the U.S., and then it had subsequently wired the transfers abroad. Pursuant to this allegation, the U.S. persuaded the relevant authorities in West Germany, Canada, and Switzerland to joint it in freezing Banco de Occidente assets, amounting to about $80 million. The frozen assets bore no relationship to the funds tainted by the money laundering activities. The U.S. justified its action on the theory that the $80 million represented substitute funds. The worldwide seizure of Banco de Occidente's funds represented approximately one half of its total assets, and the action almost immediately forced the bank into insolvency. Even though the allegedly guilty parties were two subordinate employees operating independently and without the knowledge of the banks management, the bank pleaded guilty and agreed to forfeit $5 million over a period of four years.").

162. *See* United States v. Trapilo, 130 F.3d 547, 551 (2d Cir. 1997). The court held that a scheme to defraud a foreign government of tax revenue falls within the purview of the wire fraud statute. The statute proscribed the use of telecommunications systems of the United States in furtherance of a scheme whereby one intends to defraud another of property: the identity and location of the victim, as well as the success of the scheme are irrelevant. The court found that even though the wire fraud statute could be construed less harshly, the rule of lenity was not implicated merely because the law was applied in a situation not expressly anticipated by Congress.

163. Criminal indictment filed in *United States v Banco de Occidente*, S.A, in Mar. 1989. Cited in Matthew S. Morgan, "Money Laundering: The United States Law and Its Global Influence," Essay in International Financial and Economic Law No. 5, 1996.

164. *Id.*

165. *Id.*

foreign jurisdictions.[166] Moreover, part of the exchange of real currency, drugs, and/or illegal services for Bitcon occurred in the United States.[167] As such, users of Silk Road, as well as DPR himself, would likely fall within the jurisdiction of the U.S. money laundering and wire fraud statutes, no matter where they were located.[168]

The extent to which foreign nationals may be held criminally liable in the United States under the wire fraud statute for their activities abroad is illustrated by the case *U.S. v. Chalmers*. In *Chalmers*, several defendants were indicted for wire fraud and conspiracy for bribing Iraqi government officials in exchange for the right to receive allocations of Iraqi oil under the Oil-for-Food Program.[169] The district court held that the Iraqi people were a victim as required for wire fraud, regardless of whether the people as a group were recognized as a person under international law.[170] Processing Bitcoin transactions requires the expenditure of collective resources by participants in the Bitcoin network, and fraudulent entries in the Block Chain cannot be removed.[171] As such, fraudulent use of Bitcoin imposes costs on Bitcoin Network participants indefinitely, and the ruling in *Chalmers* may provide a basis for prosecuting foreign criminals who make use of Bitcoin, even where no other obvious victim exists, because such activity defrauds Bitcoin Network participants.

B. *Vicarious Liability Under the Aiding and Abetting Statute is a Powerful Tool for Regulation of Criminal Activity Involving Bitcoin*

In addition to the extraterritorial reach of U.S. criminal law, vicarious liability may be one of the most powerful tools for regulation of

166. *See* Press Release, FBI New York Field Office, *supra* note 151.

167. *Id.*

168. At bottom, the extraterritorial applicability of the U.S. wire fraud statute is quite broad. *See* United States v. Chalmers, 474 F.Supp. 2d 555, 563-64 (S.D.N.Y. 2007). The Block Chain is actively maintained and stored by computers throughout the United States and the rest of the world. It is maintained through a peer-to-peer network that incorporates computer networks within the United States. As such, a fraud scheme facilitated by the use of Bitcoin must use the telecommunications network of United States and will thus fall within the jurisdiction of the wire fraud statute.

169. 474 F. Supp. 2d 555, 558 (S.D.N.Y. 2007).

170. *Id.* at 561.

171. *See* KEN SHIRRIFF'S BLOG, *supra* note 48 (discussing how text embedded within the block chain persists over time); Christian Decker, Roger Wattenhofery, Information Propagation in the Bitcoin Network, Proceedings of the 13th IEEE International Conference on Peer-to-Peer Computing (2013) ("In the case of transactions, stopping the propagation is a reasonable trade off, that protects the network from transaction spam, at the expense of individual users.").

criminal activity involving Bitcoin.[172] Although DPR was not charged with aiding and abetting, a person can be convicted of aiding and abetting another's violation of a statute even if it would not be possible to convict the aider and abettor as a principal.[173] The aiding and abetting statute, however, does not establish a separate offense, but rather imputes the actions of the principal to the aider and abettor as a matter of law.[174] Whether a defendant is convicted as a principal or as an accomplice does not change the underlying offense.[175] Accordingly, "it is not possible to incur criminal liability for aiding and abetting what is not a crime; no matter the government's theory of the case, some crime must be committed before criminal liability attaches."[176] Although the aiding and abetting statute does not expand the extraterritorial reach of the underlying criminal offense,[177] given the broad extraterritorial reach of the wire fraud statute, persons outside the United States who act as intermediaries for others engaged in criminal abuse of Bitcoin, such as market makers and exchangers of Bitcoin for

172. Vicarious criminal liability for coconspirators is well entrenched in federal law. For example, the conspiracy statute provides that "if two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to affect the object of the conspiracy, each shall be fined . . . or imprisoned . . . or both." 18 U.S.C.A. § 371 (West); *see also* 18 U.S.C. § 2(a) (2000) ("[w]hoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal."); United States v. Wilson, 160 F.3d 732, 738 (D.C. Cir. 1998). In the Silk Road case, DPR was indicted on counts of narcotics conspiracy, conspiracy to commit computer hacking, and money laundering conspiracy for his alleged role as the owner and operator of the site, yet the facts of the case presented by the Department of Justice suggest that the aiding and abetting statute could have been used against DPR. Press Release, FBI New York Field Office, *supra* note 51.

173. *See, e.g.*, *In re* Nofziger, 956 F.2d 287, 290 (D.C. Cir. 1992); United States v. Raper, 676 F.2d 841, 849 (D.C. Cir. 1982); *see also* Coffin v. United States, 156 U.S. 432, 447 (1895).

174. United States v. Stands, 105 F.3d 1565, 1577 (8th Cir. 1997).

175. United States v. Yielding, 657 F.3d 688 (8th Cir. 2011); United States v. Powell, 652 F.3d 702 (7th Cir. 2011).

176. Kash v. United States, 112 F. App'x. 518 (7th Cir. 2004).

177. United States v. Yakou, 428 F.3d 241, 251-54 (D.C. Cir. 2005). In *United States v. Yakou*, the court held that the aiding and abetting statute did not expand the extraterritorial reach of the Arms Export Control Act. *Id.* (referencing 22 U.S.C. § 2778(b)(1)(A)(ii)(I)). The court found that the congressional choice to limit liability to "U.S. persons" under the brokering amendment to the Act was highly significant and inconsistent with charging non-U.S. persons who engaged in brokering activities with a "U.S. person" under the aiding and abetting statute. The court in *Yakou* recognized that the actions of the defendant were no less harmful to the United States by virtue of the fact that he was not a "U.S. person," within the meaning of the act, but reaffirmed that in the absence of a clear expression of congressional intent to the contrary, the crime of aiding and abetting confers extraterritorial jurisdiction to the same extent as the offense that underlies it.

real currency, could be prosecuted under the aiding and abetting statute as if they themselves committed the crimes they facilitate.

It is less clear, however, what, if any, potential liability may exist for those who facilitated DPR's illegal enterprise by maintaining the ledger of the illicit transactions he brokered (i.e., the Block Chain). *U.S. v. Hornaday*[178] suggests that the pseudo-anonymity of Bitcoin transactions will not provide a safe harbor for such individuals, because an aiding and abetting charge could stand as long as the Silk Road users' conduct was illegal under U.S. law.[179] Accordingly, if either the users of Silk Road or DPR himself could be charged under U.S. law, then it is possible that the persons maintaining the ledger of these illicit transactions could be charged with aiding and abetting violations of U.S. law. By extension, only if the users of neither Silk Road nor DPR were subject to U.S. criminal jurisdiction would those maintaining the Block Chain be beyond the reach of charges that they aided and abetted violations of U.S. criminal law.

Even though the crime of aiding and abetting confers extraterritorial jurisdiction only to the same extent as the offense that underlies it, in the cases of aiding and abetting violations of the wire fraud or money laundering statutes (discussed in detail in the preceding section) the extent of that extraterritorial reach is vast.[180] As such, if the Bitcoin Network stratifies into classes of service, it may be possible for U.S. authorities to stem criminal abuse of the system by threatening prosecution of large-scale Bitcoin mining operations.[181] This could have the

178. United States v. Hornaday, 392 F.3d 1306 (11th Cir. 2004) (holding that liability could exist under the aiding and abetting statute for the acts of an undercover agent that are caused by the defendant, where those acts would be an offense against the United States if the defendant had done the acts himself, but that defendant, who contacted an undercover law enforcement agent in an attempt to entice a minor into unlawful sexual activity, could not be held liable under the aiding and abetting statute since the only federal crime was the one committed by defendant).

179. *Id.*

180. *Yakou*, 428 F.3d at 251-54. (finding that the congressional choice to limit liability to "U.S. persons" under the brokering amendment to the Arms Export Control Act [14] was highly significant and inconsistent with charging non-U.S. persons who engaged in brokering activities with a "U.S. person" under the aiding and abetting statute).

181. *See* Harriet Agnew, *Famed Trader Backs Bitcoin*, WJS ONLINE (Aug. 3, 2013) (*available at* http://online.wsj.com/news/articles/SB20001424127887323997004578644491403250124) (last accessed 4/28/2014); *see also* Nathaniel Popper, *Into the Bitcoin Mines*, N.Y. TIMES, Dec. 21, 2013 (discussing a rather elaborate, and one might assume expensive, bitcoin mining setup) ("To get [to a bitcoin mining operation in Iceland], you pass through a fortified gate and enter a featureless yellow building. After checking in with a guard behind bulletproof glass, you face four more security checkpoints, including a so-called man trap that allows passage only after the door behind you has shut. This brings you to the center of the operation, a fluorescent-lit room with

effect of spurring a process of setting standards and compliance efforts that may also address concerns raised by FinCEN in its guidance memorandum. In particular, this threat of prosecution could encourage Bitcoin MSBs to better know who they are servicing and take measures to ensure compliance with U.S. money laundering and anti-terrorism laws.

C. *The Structure of the Bitcoin Network is Particularly Suitable to Conspiracy Prosecutions*

The structure of the Bitcoin Network is particularly suitable to conspiracy sting investigations and prosecutions under the federal conspiracy statute.[182] A "conspiracy participant is legally liable for all reasonably foreseeable acts of his or her co-conspirators in furtherance of the conspiracy."[183] A criminal conspiracy under U.S. law requires at least two parties having the requisite mens rea, but the parties to the conspiracy can be brought together by a third party working on behalf of the U.S. government.[184] Even though it is impossible to conspire with an undercover agent or informer, this must be distinguished from instances where a valid agreement exists between two or more conspirators, one of whom commits overt acts solely with a government agent.[185]

more than 100 whirring silver computers, each in a locked cabinet and each cooled by blasts of Arctic air shot up from vents in the floor.").

182. *See* 18 U.S.C.A. § 371 (West).

183. United States v. Brewer, 983 F.2d 181, 185 (10th Cir.1993) (citing Pinkerton v. United States, 328 U.S. 640 (1946); United States v. Kissel, 218 U.S. 601, 608 (1910)).

184. Under 18 U.S.C. § 371, an agreement between only two actors, one of whom is a government agent, cannot support a conspiracy conviction. *See* United States v. Dimeck, 24 F.3d 1239, 1242 n.6 (10th Cir. 1994) ("[c]onfidential informants and government agents cannot serve as the second party to a conspiracy."); United States v. Barger, 931 F.2d 359, 369 (6th Cir. 1991) (holding that conspiracy cannot be proven between defendant and government agent); United States v. Vasquez, 874 F.2d 1515, 1516-17 (11th Cir. 1989); United States v. Manotas-Mejia, 824 F.2d 360, 364-65 (5th Cir. 1987); *see also* United States v. Ritter, 989 F.2d 318, 321 (9th Cir. 1993) (finding no conspiracy to violate 18 U.S.C. § 1958 when only co-conspirators were government agents). Section 371 requires a bilateral conspiracy; an agreement between two or more bona fide conspirators is a necessary element of the crime. 18 U.S.C.A. § 371 (West). Because the government must prove that at least two culpable parties, including the defendant, reached an agreement, proof of an agreement solely between a defendant and a government agent or informer will not support a conspiracy conviction. Rogers v. United States, 340 U.S. 367, 375 (1951); Morrison v. California, 291 U.S. 82, 92 (1934); United States v. Giry, 818 F.2d 120, 125 (1st Cir. 1987); United States v. Escobar de Bright, 742 F.2d 1196, 1199-1200 (9th Cir. 1984); United States v. Pennell, 737 F.2d 521, 536 (6th Cir. 1984); United States v. Barnes, 604 F.2d 121, 161 (2d Cir. 1979); United States v. Chase, 372 F.2d 453, 459 (4th Cir. 1967).

185. United States v. Enstam, 622 F.2d 857, 867 (5th Cir. 1980).

For example, the court in *United States v. Jordan* upheld the liability of a co-conspirator for causing the unlawful importation of heroin under such a theory, where an undercover government agent carried out the actual act of importation.[186] The *Jordan* court held that the actions of the defendant's co-conspirator, causing an agent to commit an offense in furtherance of the conspiracy, were reasonably foreseeable.[187] Thus, a government agent can serve as a link between two true conspirators.[188] As such, a government agent brokering Bitcoin transactions through a site similar to Silk Road could ensnare criminals with the promise of anonymity, while in reality laying the foundation for criminal charges based upon the jurisdictional hook arising from the use of Bitcoin in criminal transactions.

If a criminal conspiracy utilizes Bitcoin, those who join in the conspiracy may be subject to prosecution even though their individual conduct occurred outside of the United States at the behest of a U.S. government agent and even if the only overt act was carried out by a government agent.[189] This liability, however, arises under the conspiracy statute itself, not the money laundering or wire fraud statutes.[190] In this respect, the conspiracy statute offers something the aiding and abetting statute cannot: a means to punish a foreign national operating abroad as part of a criminal conspiracy that utilizes the Bitcoin Network, regardless of whether any substantive violation could be proved.

D. *International Discovery Devices Extend the Reach of Law Enforcement Authorities Combating Criminal Abuse of Bitcoin*

In addition to the broad extraterritorial application of U.S. criminal laws, enforcement agencies can also utilize international discovery devices under 18 U.S.C.A. § 3292 to extend the statute of limitations applicable to those criminally abusing Bitcoin. For example, if DPR had hosted the Silk Road site in a country other than the United States or maintained his Bitcoin wallet abroad, the statute of limitations under U.S. criminal law could have been suspended while necessary evidence

186. United States v. Jordan, 927 F.2d 53, 56 (2d Cir. 1991).

187. *Id.*

188. *See* United States v. Fincher, 723 F.2d 862, 863 (11th Cir. 1984) (holding that an agent may "link" genuine conspirators) (citing Sears v. United States, 343 F.2d 139, 142 (5th Cir. 1965)).

189. *See* Ford v. United States, 273 U.S. 593, 620 (1927).

190. *See id.*

was requested from one or more foreign governments.[191] Accordingly, neither time nor distance presents much of an impediment to U.S. federal prosecutors. In cases relying upon the extraterritorial application of U.S. law, the period of tolling the statute of limitations may be extended, and, therefore, the potential for criminal liability for those using the Bitcoin Network for illegal purposes may follow them for some time. While such an extension was apparently unnecessary in the case of the Silk Road defendants, it could become a useful tool for U.S. prosecutors investigating crimes involving Bitcoin in which criminals, perhaps learning from DPR's mistakes in the Silk Road Case, attempt to evade U.S. criminal jurisdiction.

Furthermore, given the emerging and evolving nature of the criminal case law involving Bitcoin, the government may further extend the statute of limitations in such cases by, for example, making additional official requests.[192] As the types and forms of evidence relied upon in future U.S. criminal prosecutions of Bitcoin-related crimes change with the technology, so too can the requests for evidence that will keep such

---

191. *See* United States v. Jenkins, 633 F.3d 788, 802 (9th Cir. 2011) (holding government's June 20, 2005 application was sufficient to suspend the statute of limitations for all counts, effective March 16, 2005). In *United States v. Jenkins*, the defendants were convicted in the United States District Court for the District of Arizona of multiple counts of fraud and money laundering. *Id.* at 796. They appealed on several grounds, including that § 3292 does not permit the district court to suspend the statute of limitations if the government applies for an extension after the statute has expired, and that the government's submission of its official request for evidence to a foreign government before the expiration of the statute is irrelevant. *Id.* at 797. The court rejected these arguments, ruling that the only temporal requirements of an application for suspension of a statute of limitations to permit the government to obtain foreign evidence under the statute are: (1) that the official request for evidence in a foreign country be made before the statute of limitations expires; and (2) that the application for suspension be submitted to the district court before the indictment is filed. *Id.* at 799; *see also* United States v. Daniels, C 09-00862 MHP, 2010 WL 2680649 at *7 (N.D. Cal. July 6, 2010) (finding that an indictment was filed within the statute of limitations because a "section 3292 order" was valid).

192. *See* United States v. Hagege, 437 F.3d 943, 955 (9th Cir. 2006). In *United States v. Hagege*, the defendant was convicted in the United States District Court for the Central District of California of bankruptcy fraud and false representation of a Social Security number. *Id.* at 946. The United States Court of Appeals for the Ninth Circuit found that the Israeli government's letter, stating "in the future, should you need certified copies of the bank statements, please let me know," was not a disposition of the U.S. certification request, and thus the Israeli government did not take final action on the certification request until it sent the requested certificate of authenticity. *Id.* at 954, 956. The court held that 18 U.S.C. § 3292 directed the District Court to suspend the running of the statute of limitations while the government's official request for evidence in a foreign country was pending, and the government was not prohibited from extending the suspension period by making an official request for certified documents with a future delivery provision. *See id.* at 956.

prosecutions alive. So long as prosecutors remain abreast of the technology, Bitcoin criminals cannot rely upon technological advances to run the clock out on the statute of limitations.

E. *Recent Guidance on the Tax Status of Virtual Currency Issued by the U.S. Internal Revenue Service May Significantly Enlarge the Population of Bitcoin Users Subject to Criminal Prosecution*

Bitcoin transactions are taxable in the United States. The U.S. Revenue Code provides that except as otherwise provided in law, gross taxable income includes all income from whatever source derived, including, one would presume, Bitcoin.[193] Indeed, on March 25, 2014, the U.S. Internal Revenue Service (IRS) issued an "IRS Virtual Currency Guidance" memorandum, which lays out the agency's position on the taxation of virtual currencies such as Bitcoin.[194] The position taken by the IRS may significantly enlarge the population of Bitcoin users that are subject to U.S. criminal prosecution. If this risk materializes, it could have a significant chilling effect on the available supply of Bitcoin, the sustainability of mining cooperatives, and the wider adoption of Bitcoin generally.

First, the IRS has adopted the position that Bitcoin miners are engaged in the trade or business of producing Bitcoin and thus the proceeds derived from the sale or exchange of Bitcoin they mine are taxable as ordinary income.[195] This is significant because without careful accounting of the electricity and amortized computational resources expended to mine Bitcoin, most miners will find that tax is due on the full market value of the Bitcoin they mine. Second, much of the Bitcoin that has been mined to date remains tightly held by early

193. *See* 26 U.S.C.A. 61(a) (West).

194. IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes, General Rules for Property Transactions Apply, IR-2014-36, INTERNAL REVENUE SERVICE (Mar. 25, 2014) *available at* http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance (announcing that wages paid to employees using virtual currency are taxable to the employee, must be reported by an employer, and are subject to federal income tax withholding and payroll taxes, that payments using virtual currency made to independent contractors and other service providers are taxable and self-employment tax rules generally apply, and that Bitcoin is treated as property for federal tax purposes, and, as such, the character of gain or loss from the sale or exchange of virtual currency depends on whether it is a capital asset in the hands of the taxpayer and on the taxpayer's taxable basis in the Bitcoin; announcing that the position of the IRS is that Bitcoin acquired in an exchange for goods or services has a taxable basis equal to the market price at the time of the exchange, and Bitcoin that is purchased has a taxable basis equal to the purchase price).

195. *Id.*

adopters that have little or no taxable basis under the IRS's approach. Thus, the IRS rules effectively make transactions by such early Bitcoin adopters taxable at a 10-39.6% rate.[196] By extension, these rules will likely impose burdensome taxation and reporting requirements on participants in mining pools, as well as many other individuals who are unlikely to report their transactions and pay the taxes due.

Tax evasion is a crime under U.S. law punishable by a fine and/or imprisonment.[197] Section 7201 of the IRS Code creates two offenses: (a) the willful attempt to evade or defeat the assessment of a tax and (b) the willful attempt to evade or defeat the payment of a tax.[198] Passive failure to file tax returns, however, is not tax evasion.[199] Moreover, a defendant's good faith belief that he is not violating the tax laws, no matter how objectively unreasonable that belief may be, is a defense in a tax prosecution.[200] But the failure to file a return coupled with an affirmative act of evasion, commonly referred to as a "*Spies* evasion," is subject to prosecution.[201] Moreover, a defendant's erroneous belief that tax laws are unconstitutional is no defense to tax evasion.[202] Indeed, the timing of the recently issued IRS guidance suggests an effort to remove any ambiguity as to whether Bitcoin transactions generate taxable income, but it remains to be seen whether taxable Bitcoin transactions will be self-reported.

If those engaging in Bitcoin transactions fail to file a return, an evasion case can be maintained only if it can be shown that the taxpayer engaged in an affirmative act to conceal or mislead.[203] The Supreme Court in *Spies* noted, however, that concealing sources of income,

196. *See* Kelly Phillips, *IRS Announces 2014 Tax Brackets, Standard Deduction Amounts And More*, FORBES (Oct. 31, 2013), http://www.forbes.com/sites/kellyphillipserb/2013/10/31/irs-announces-2014-tax-brackets-standard-deduction-amounts-and-more/ (last visited May 3, 2014).

197. I.R.C. § 7201 ("Any person who willfully attempts in any manner to evade or defeat any tax imposed by this title or the payment thereof shall, in addition to other penalties provided by law, be guilty of a felony and, upon conviction thereof, shall be fined* not more than $100,000 ($500,000 in the case of a corporation), or imprisoned not more than 5 years, or both, together with the costs of prosecution.").

198. *Id.*; Sansone v. United States, 380 U.S. 343, 354 (1965); United States v. Mal, 942 F. 2d 682, 687-88 (9th Cir. 1991) (finding that if a defendant transfers assets to prevent the IRS from determining his true tax liability, he has attempted to evade assessment; if he does so after a tax liability has become due and owing, he has attempted to evade payment.).

199. I.R.C. § 7201.

200. Cheek v. United States, 498 U.S. 192, 199-201 (1991); *see also* United States v. Grunewald, 987 F.2d 531, 535-36 (8th Cir. 1993); United States v. Pensyl, 387 F.3d 456, 459 (6th Cir. 2004).

201. Spies v. United States, 317 U.S. 492, 498-99 (1943).

202. Cheek v. United States, 498 U.S. 192, 205-06 (1991).

203. Spies, 317 U.S. at 498-99.

handling transactions in a manner that avoids creating the usual records, as well as any other conduct likely to conceal or mislead, may satisfy the affirmative act requirement.[204] Moreover, under the *Spies* ruling, the willfulness prong of the tax evasion test may be inferred from "any conduct, the likely effect of which would be to mislead or to conceal."[205] Courts have found that extensive use of currency and cashier's checks,[206] engaging in surreptitious transactions using cash, money orders, or cashier's checks,[207] holding bank accounts under fictitious names,[208] and handling one's affairs to avoid making the usual records required for such transactions[209] were each sufficient to infer willfulness. The very use of Bitcoin arguably makes it easier to prove any or all of these indicia of a willful affirmative act, and thus the use of Bitcoin makes tax payers especially vulnerable in a tax evasion prosecution.

As FinCEN notes in its recently issued regulations,[210] the use of Bitcoin bears several similarities to the use of cash, money orders, or cashier's checks. Moreover, the Bitcoin network is arguably designed to avoid creating the usual records and conceal the identity of all parties to a transaction. Indeed, many early adopters of virtual currency, often miners themselves, were attracted to its use in the first place because they wanted to create a currency that circumvents both the government and taxes.[211] Moreover, the fact that Bitcoin wallets are pseudo-anonymous— being identified solely by a binary address—arguably

204. *Id.*

205. *Id.*

206. United States v. Daniel, 956 F.2d 540, 543 (6th Cir. 1992); United States v. Holovachka, 314 F.2d 345, 357-58 (7th Cir. 1963); Schuermann v. United States, 174 F.2d 397, 398 (8th Cir. 1949).

207. United States v. Kim, 884 F.2d 189, 192-93 (5th Cir. 1989); United States v. Skalicky, 615 F.2d 1117, 1120 (5th Cir. 1980); United States v. Holladay, 566 F.2d 1018, 1020 (5th Cir. 1978); United States v. Mortimer, 343 F.2d 500 (7th Cir. 1965).

208. United States v. Ratner, 464 F.2d 101, 105 (9th Cir. 1972); Elwert v. United States, 231 F.2d 928, 936 (9th Cir. 1956).

209. United States v. Dowell, 446 F.2d 145, 147 (10th Cir. 1971); Gariepy v. United States, 189 F.2d 459, 463 (6th Cir. 1951).

210. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (March 18, 2013); DEPT. OF TREASURY, *supra* note 11.

211. *See* Josh Ritchie, *Bitcoins: The Taxless Currency*, TURBOTAX BLOG (July 18, 2011), http://blog.turbotax.intuit.com/2011/07/18/bitcoins-the-taxless-currency/ (explaining that because income derived from a virtual currency exchange is declared only through an honor system, some people may be attracted to bitcoin because they want to avoid taxes).

weighs in favor of the IRS in an evasion prosecution.[212] Furthermore, even if the use of Bitcoin by a particular person serves purposes other than evading taxes, e.g., to remit funds oversees, if a tax evasion motive plays *any part* in defendant's conduct, the offense of tax evasion may be made out even though the conduct may also serve purposes other than tax evasion.[213] Additionally, officers of businesses that mine Bitcoin may be criminally liable for any deficiency in taxes paid by the business.[214] As such, the imposition of high income tax levels on mining activity should be of concern not only to mining pool participants, solo mining operations, exchanges, and other MSB's defined under the recent FinCEN guidance, but also to users of Bitcoin more generally.[215]

Since the IRS rules make many reported transactions in Bitcoin taxable at ordinary income rates, it is likely that many users of the virtual currency will simply not file the required returns. Therefore, the IRS rules will likely drive Bitcoin further into the shadows and increase its ties to criminal activity. Moreover, the approach adopted by the IRS also threatens to create a "lock out" effect that could severely impact the supply of Bitcoin available for conducting transactions within the United States.[216] Tax evasion may offer law enforcement officials another tool in their pocket when attempting to charge criminals who also use Bitcoin; however, by creating a profitable opportunity for tax arbitrage (i.e., "off-shoring" of Bitcoin and the profits associated with its use, criminal or otherwise) the IRS may be undermining the ability

---

212. Holding property in nominee names can satisfy the affirmative act requirement. United States v. Schoppert, 362 F.3d 451, 460 (8th Cir. 2004); United States v. Wilson, 118 F.3d 228, 236 (4th Cir. 1997); United States v. Peterson, 338 F.2d 595, 597 (7th Cir. 1964). Concealment of bank accounts can satisfy the affirmative act requirement. Wilson, 118 F.3d at 236; Paschen v. United States, 70 F.2d 491 (7th Cir. 1934); United States v. Carlson, 235 F.3d 466, 469 (9th Cir. 2000) (using a false SSN on bank accounts).

213. United States v. Voigt, 89 F.3d 1050, 1090 (3d Cir. 1996).

214. United States v. Troy, 293 U.S. 58, 59 (1934); United States v. Aracri, 968 F.2d 1512, 1523 (2d Cir. 1992); United States v. Frazier, 365 F.2d 316, 318 (6th Cir. 1966); Tinkoff v. United States, 86 F.2d 868, 876 (7th Cir. 1937).

215. *See* Jose Paglier, *New IRS rules make using Bitcoins a fiasco*, CNN MONEY (Mar. 31, 2014), http://money.cnn.com/2014/03/31/technology/irs-bitcoin/.

216. *See*, John R. Graham et al., *Barriers to Mobility: The Lockout Effect of U.S. Taxation of Worldwide Corporate Profits*, 63 NATL. TAX J. 1111-1144 (Dec. 2010) (presenting a study of the incentives firms face when deciding whether to repatriate earnings back to the United States and the effects of U.S. tax policy on capital mobility); Melissa Redmiles, *The One-Time Dividend Received Deduction*," INTERNAL REVENUE SERV. (Working Paper, 2007) (estimating that the temporary deduction of 85% on foreign earnings repatriated back to the United States provided by the American Jobs Creation Act of 2004 stimulated the repatriation of more than $300 billion in foreign-earned dividend income).

of U.S. law enforcement officials to pursue more nefarious activities. As such, despite the considerable thought given by U.S. authorities and private citizens to the appropriate approach to taxing virtual currencies,[217] the result of the approach adopted by the IRS could be an increase in criminal abuse sheltered in low-tax jurisdictions and a stifling effect on Bitcoin adoption by legitimate users due to price inflation and limited supply.

VI. Conclusion

The international regulatory landscape for Bitcoin is a patchwork of inconsistent and incomplete attempts to counter criminal abuse of the technology. In order to realize this technology's transformative potential, it is essential that its criminal abuse be dealt with effectively. The U.S. Criminal Code contains a set of tools that may be extremely effective in the absence of a more coordinated international framework, but with respect to the U.S. approach to taxing Bitcoin transactions, there are areas in significant need of improvement. Bitcoin's potential to improve the lives of the world's poor and disadvantaged justifies both reworking the tax code in order to foster Bitcoin's development and adopting the robust extraterritorial application of the U.S. Criminal Code to help mitigate the risks posed by disintermediation of the financial services industry.

217. *See, e.g.*, GAO Report *supra*, note 9 (discussing unanswered questions and misinformation available on the Internet); *see also Tax Compliance*, Bitcoin Wiki, https://en.bitcoin.it/wiki/Tax_compliance; *Bitcoin accounting and taxes*, Bitcoin Forum, https://bitcointalk.org/index.php?topic=14334.0; *CM#1001: Staying Between the Lines: A Survey of U.S. Income Taxation and its Ramifications on Cryptocurrencies*, Cryptocurrency Legal Advocacy Group, http://theclag.org/CM%231001Final.pdf; Trace Mayer, A Lawyer's Take on Bitcoin and Taxes (1st ed. 2012).

THE BLOCK IS HOT: A SURVEY OF THE STATE OF BITCOIN REGULATION AND SUGGESTIONS FOR THE FUTURE

Misha Tsukerman†

Bitcoin, the famous and sometimes infamous digital currency, has two key uses. First, it can serve as a currency to buy and sell goods and services.[1] Second, as its value has fluctuated dramatically within recent years, many users purchase Bitcoins for speculative purposes.[2] Bitcoin exists wholly as lines of computer code[3] governed by the Bitcoin protocol, the program that dictates the generation and transfer of Bitcoins.[4] Unlike fiat currencies such as the U.S. dollar ("USD"), Japanese yen, or euro, Bitcoin is not backed by the government of any nation or by a physical commodity such as gold.[5] Instead, the value of Bitcoin is based on the trust people put in it and its scarcity.[6] In 2013, the market price of a single Bitcoin ranged from thirteen to 1200 USD.[7] Bitcoin relies on cryptography[8] to validate and govern its production and use, with each transaction recorded on an online public ledger called the "blockchain."[9]

---

† J.D. Candidate, 2016, University of California, Berkeley, School of Law.

1. Matthew Kien-Meng Ly, *Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J.L. & TECH. 587, 591 (2014).

2. CRAIG K. ELWELL ET AL., CONG. RESEARCH SERV., BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 1 at 6 (2014).

3. Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV 111, 116 (2012).

4. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG (Nov. 8 2008), https://bitcoin.org/bitcoin.pdf (Satoshi Nakamoto is not necessarily one person or an actual name. *See infra* note 34.).

5. Kaplanov, *supra* note 3, at 115.

6. *See* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCIENCE & TECH. L.J. 159, 168, 175 (2012)(noting that confidence in Bitcoin as a limited resource is integral to the value of Bitcoin).

7. Ly, *supra* note 1 at 591.

8. Cryptography is more generally the "process of writing or reading secret messages or codes." *Cryptography Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/cryptography (last visited Nov. 26, 2014).

9. Nakamoto, *supra* note 4.

Virtual currencies such as Bitcoin were not viable in the past because of the "double-spending" problem, where an owner of a digital currency file could easily make an exact copy of that file and send it to more than one person.[10] A currency that is non-rivalrous and can be held at the same time by more than one user is valueless.[11] What makes Bitcoin, the most popular virtual currency,[12] rivalrous and scarce is that it can only be transferred within the blockchain.

The blockchain is a privately operated and completely decentralized system, requiring no traditional financial institution or central controlling entity for transactions.[13] The blockchain acts as an online record keeping system that tracks the ownership of specific Bitcoins from their creation (in a process called mining)[14] through every subsequent transaction.[15] The blockchain does not exist in a central location, but rather through a peer-to-peer ("P2P") network[16] composed of all Bitcoin users.[17] Bitcoin "miners" use their computer's processing power to maintain the Bitcoin network, and are rewarded in Bitcoins through the Bitcoin protocol.[18]

---

10. JERRY BRITO & ANDREA CASTILLO, BITCOIN, A PRIMER FOR POLICYMAKERS 3–4, (Mercatus Center 2013).

11. Josh Fairfield, *BitProperty*, 88 S. CAL. L. REV. at 15 (forthcoming 2015), *available at* http://ssrn.com/abstract=http://ssrn.com/abstract=2504710.

12. *See* CoinMarketCap, *infra* note 59 (showing Bitcoin's market capitalization over seven times higher than the next most popular virtual currency). Bitcoin is also the only virtual currency to have an NCAA football game named after it. In an effort to move the chains of public perception, the Bitcoin payments firm BitPay sponsored the St. Petersburg Bowl between North Carolina State University and the University of Central Florida on December 26, 2014. Formerly the "Beef 'O' Brady Bowl," tickets and merchandise at the "Bitcoin St. Petersburg Bowl" game could be purchased with Bitcoin. *See* Michael J. Casey, *BitPay to Sponsor St. Petersburg Bowl in First Major Bitcoin Sports Deal*, WALL ST. J. (June 18, 2014), http://www.wsj.com/articles/bitpay-to-sponsor-st-petersburg-bowl-in-first-major-bitcoin-sports-deal-1403098202.

13. ELWELL ET AL., *supra* note 2, at 1

14. Discussed *infra* Section I.B.

15. ELWELL ET AL., *supra* note 2, at 3.

16. A P2P network is a "network of personal computers, each of which acts as both client and server, so that each can exchange files . . . with every other computer on the network." *Peer-to-peer Network Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/peer-to-peer%20network (last visited Nov. 28, 2014). This is different from a client/server network where "one centralized, powerful computer (called the server) is a hub to which many less powerful personal computers . . . (called clients) are connected. The clients run programs and access data that are stored on the server." *Server Network Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/client/server%20network (last visited Nov. 28, 2014).

17. Fairfield, *supra* note 11, at 18 (the blockchain is a decentralized and distributed list).

18. Nakamoto, *supra* note 4.

Thus, no particular party can be said to "control" the blockchain. Profits realized from mining Bitcoin and transaction fee commissions in Bitcoin remain the key incentives for maintenance of the blockchain.[19]

The promise of the blockchain as a decentralized trustless public ledger extends far beyond simply tracking different Bitcoins. The true technological revolution the blockchain represents is the creation of a system that for the first time allows for scarce, rivalrous digital property.[20] The blockchain is prohibitively difficult to hack and falsify and could be used as a reliable system to track the ownership of real property, such as land deeds or automobiles, drastically lowering search and transaction costs.[21] The blockchain has even been suggested as a system to prevent voter fraud.[22] Yet, for these gains to be fully realized, and for the benefits of the network effect,[23] there must be broader adoption of Bitcoin by the general public. Bitcoin will have to come out of the shadows and be seen and used by the general public for more than speculation and the online purchase of drugs and other contraband.[24]

As Josh Fairfield observes,[25] the blockchain "is not financial, it is not asset-based, it is not insurance, or securities, or any one of a number of uses. . . . [It] is simply a protocol for tracking information about rivalrous digital interests."[26] Thus, this Note posits that the job of regulators is to allow the blockchain to thrive and allow for consumer confidence in its potential to create a safe and reliable system of public records to allow for the safe transfer of real property.

---

19. Fairfield, *supra* note 11, at 19.

20. *See id.* at 5.

21. *See generally* Fairfield, *supra* note 11.

22. *See generally* Matt Odell, *How Bitcoin Could Make Voter Fraud and Stolen Elections Impossible*, ENTREPRENEUR (Nov. 20, 2014), http://www.entrepreneur.com/article/239809.

23. "A product displays positive network effects when more usage of the product by any user increases the product's value for *other* users (and sometimes all users)." Arun Sundarajan, *Network Effects*, @DIGITALARUN, http://oz.stern.nyu.edu/io/network.html (last visited Feb. 10, 2015).

24. *Infra* Section III.A.

25. Professor Fairfield is an internationally recognized law and technology scholar. Professor Fairfield specializes in digital property, electronic contracts, big data privacy, and virtual communities. *See* Biography of Professor Joshua A.T. Fairfield, WASHINGTON AND LEE UNIVERSITY SCHOOL OF LAW, http://law2.wlu.edu/faculty/profiledetail.asp?id=242 (last visited Feb. 25, 2015).

26. Fairfield, *supra* note 11, at 67.

Trust in a currency is essential to its adoption[27] and while Bitcoin can provide many benefits over cash and credit card transactions,[28] virtual currency, like all digital technologies is capable of massive and systemic failure.[29] This current age is one of massive cyber intrusions and hacks.[30] Even the economic collapse in 2008 was partly driven by technological failure.[31] While the Bitcoin protocol's technical features create an inherent level of security,[32] it is, of course, the risks that have not yet been imagined that are the most dangerous. Unlike with cash, an undiscovered vulnerability in the Bitcoin protocol could lead to catastrophic failure of the entire Bitcoin ecosystem. Preventing and mitigating these risks will require smart, flexible, and active regulation. This regulation must be balanced against concerns over stifling innovation. As with the internet, regulators must strike a balance between protecting the public from Bitcoin's bad actors, while allowing people to experiment with, and develop the technology.[33]

This Note first examines the history of Bitcoin and the mechanics of the Bitcoin protocol and the blockchain in Part I. Part II then discusses some of the potential uses of Bitcoin, from its potential as a currency, to the use of the blockchain to track other property interests. Part III examines some of risks associated with Bitcoin, from its use in online

27. *See* Supriya Singh, *Electronic Commerce and the Sociology of Money*, 4 SOCIOLOGICAL RESEARCH ONLINE 3.4 (Feb. 29, 2000), http://www.socresonline.org.uk/4/4/singh.html.

28. *See infra* Part II.

29. *See, e.g.*, Bent Flyvbjerg & Alexander Budzier, *Why Your IT Project May Be Riskier Than You Think*, HARV. BUS. REV. (Sep. 2011), https://hbr.org/2011/09/why-your-it-project-may-be-riskier-than-you-think/ (discussing the frequency with which large IT projects fail on a massive scale); Eric Scigliano, *10 Technology Disasters*, MIT TECH. REV. (June 1, 2002), http://www.technologyreview.com/featuredstory/401465/10-technology-disasters/ (highlighting the factors that consistently cause new technologies to fail).

30. *See, e.g.*, ASSOCIATED PRESS, *Sony Hack Adds to Security Pressure on Companies*, N.Y. TIMES (Dec. 19, 2014), http://www.nytimes.com/aponline/2014/12/19/world/asia/ap-as-sony-hack-company-security.html; Nicole Perlroth, *Target Struck in the Cat-and-Mouse Game of Credit Theft*, N.Y. TIMES (Dec. 19, 2013), http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html.

31. *See* Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 675 (2009).

32. *See infra* Section I.B.1.

33. *See* Mohit Kaushal & Sheel Tyle, *The Blockchain: What it is and Why it Matters*, BROOKINGS INSTITUTION (January 13, 2015), http://www.brookings.edu/blogs/techtank/posts/2015/01/13-blockchain-innovation-kaushal (noting that regulators recognized the unique nature of internet required light regulation to not stifle innovation).

black markets, the consumer protection risks to users, and Bitcoin's potential as a tax evasion mechanism. Part IV analyzes the current regulatory environment for Bitcoin and Bitcoin's role in criminal litigation. Finally, Part V suggests policy changes to disclosure requirements and tax classifications to facilitate the broader adoption of Bitcoin as a currency by the general public.

I. THE BASICS OF BITCOIN AND THE BLOCKCHAIN

This Section will describe what Bitcoins are, how the blockchain solves the double-spending problem, the security features inherent in the Bitcoin protocol, Bitcoin mining, and the blockchain as a public ledger.

A. BITCOIN BASICS

Satoshi Nakamoto, a pseudonym of a computer programmer or group of programmers,[34] proposed Bitcoin in a 2008 white paper as an open source, peer-to-peer, digital currency.[35] Bitcoins are computer files, like mp3s and gifs, and are stored in a program called a "wallet"[36] or on an online service such as Coinbase.[37] Bitcoin wallets can be held on the hard drive of a user's personal computer or on an external hard drive.[38] Like

34. In 2014, Newsweek reporter Leah McGrath Goodwin believed that she had found Bitcoin's founder in Dorian Satoshi Nakamoto in Temple City, California. Dorian Nakamoto, a former electrical engineer, has categorically denied that he is the founder of Bitcoin. *See* Leah McGrath Goodwin, *The Face Behind Bitcoin*, NEWSWEEK (March 6, 2014), http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html. The day after the story broke, the Satoshi Nakamoto account made its first post since announcing Bitcoin on the P2P Foundation Website, stating that he or she (or they) were not Dorian Nakamoto. This was the first post by the Satoshi Nakamoto account in over five years, and the mystery continues. *See* Satoshi Nakamoto, Reply to discussion titled *Bitcoin open source implementation of P2P currency* (Mar. 7, 2014), http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A52186.

35. Nakamoto, *supra* note 4.

36. Kaplanov, *supra* note 3, at 116, 124.

37. COINBASE, https://www.coinbase.com/ (last visited Feb. 10, 2015).

38. *See* CFPB, *Risks to consumers posed by virtual currencies*, at 4 (Aug. 2014), http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf (private keys can be stored on external hard drives). Dutch Bitcoin enthusiast and entrepreneur Martijn Wismeijer has implanted two microchips into his palms to keep his Bitcoin wallet handy. Cyrus Farivar, *Man has NFC chips injected into his hands to store cold Bitcoin wallet*, ARS TECHINCA (Nov. 15, 2014), http://arstechnica.com/business/2014/11/man-has-nfc-chips-injected-into-his-hands-to-store-cold-bitcoin-wallet/.

cash, Bitcoins can be destroyed, lost, or stolen.[39] For instance, if a user had their Bitcoins stored on a computer that became inoperable after being dropped, or an external hard drive storing Bitcoins was lost,[40] those Bitcoins would be irretrievable.[41] Bitcoins can only be sent or received by logging the transaction on the public ledger, the aforementioned blockchain.[42]

Bitcoins lack intrinsic value and do not derive value from a government; rather, a Bitcoin's value is purely a function of supply and demand.[43] Unlike paper "fiat currency"[44] that derives value from a government, Bitcoin is neither the creation of, nor backed by, any government.

Bitcoins can be obtained in three ways: (1) in exchange for conventional money in person or on an online exchange, (2) in exchange for the sale of goods or services, and (3) through mining.[45] Mining uses a computer's processing power to solve complex math problems both to maintain the blockchain public ledger and to "discover" new Bitcoins.[46]

Initially, Bitcoin appealed to a core group of anti-establishment enthusiasts on the fringes of the financial system, but more recently Bitcoin has become popular among venture capitalists and investment firms anticipating the wider adoption of the currency.[47] A number of leading retail businesses including Expedia, Overstock, Newegg, and the

---

39. *See* Grinberg, *supra* note 6, at 180 (2012).

40. U.K. Resident James Howell threw out an external hard drive in 2013 containing 7,500 Bitcoins. At the time, collectively these Bitcoins were valued at $9 million dollars. Kelly Phillips Erb, *From Treasure To Trash: Man Tosses Out Bitcoin Wallet On Hard Drive Worth $9 Million*, FORBES (Nov. 30, 2013), http://www.forbes.com/sites/kellyphillipserb/2013/11/30/from-treasure-to-trash-man-tosses-out-bitcoin-wallet-on-hard-drive-worth-9-million/.

41. *See* CFPB, *supra* note 38, at 4.

42. Kaplanov, *supra* note 3, at 116.

43. *Id.* at 115. Or as venture capitalist Marc Andreessen argues: "It's not as much that the Bitcoin currency has some arbitrary value and then people are trading with it; it's more that people can trade with Bitcoin (anywhere, everywhere, with no fraud and no or very low fees) and as a result it has value." Marc Andreessen, *Why Bitcoin Matters*, N.Y. TIMES (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.

44. *Fiat Money Definition*, DICTIONARY.COM http://dictionary.reference.com/browse/fiat+money (last visited on Jan. 24, 2015).

45. ELWELL ET AL., *supra* note 2, at 2.

46. *Id.*

47. Sydney Ember, *New York Proposes First State Regulations for Bitcoin*, N.Y. TIMES (July 17, 2014), http://dealbook.nytimes.com/2014/07/17/lawsky-proposes-first-state-regulations-for-bitcoin/.

Dish Network now accept Bitcoin.[48] Merchants such as Overstock deal with the price volatility of Bitcoin by immediately converting their Bitcoin revenue into dollars or some other more stable currency.[49] Overstock CEO Patrick Byrne has explained that "[u]ntil [Overstock] can hedge [the pricing risks] through some kind of derivative instrument, [the company doesn't] want to take that direct exposure."[50]

Bitcoin protocol seeks to solve the double-spending problem inherent in noncash payment systems and the need for a trusted third party (such as a bank or credit card company) to verify the integrity of the transaction.[51] There is no double-spending with cash, as the physical dollar bill must be surrendered. In a traditional noncash payment system a trusted intermediary, such as a bank or credit card company, maintains a private ledger to track account balances and prevent the double-spending.[52]

The double-spending problem is a specific version of the duplication problem, which has plagued the creation of rivalrous digital assets such as scarce digital property and currency.[53] The duplication problem occurs when an owner of a digital asset, such as an mp3, can simply duplicate the file at nearly zero cost (besides the cost of the electricity powering the computer) and thus transfer the file without losing possession of it.[54] Before the advent of the blockchain, *A* could pay both *B* and *C* with Bitcoin *X*. Something that can be sold without actually giving up possession loses much, if not all of its value.

The Bitcoin protocol solves this by making the blockchain the only way to transfer Bitcoins. Every Bitcoin transaction is broadcast to the entire network of Bitcoin users and the specific Bitcoin is assigned to a new owner on the public ledger.[55] Once a transaction has been broadcast,

48. *See, e.g.*, Shawn Knight, *Dell joins the growing list of major retailers now accepting Bitcoins*, TECHSPOT (July 18, 2014), http://www.techspot.com/news/57461-dell-joins-the-growing-list-of-major-retailers-now-accepting-bitcoins.html.

49. Rob Wile, *Bitcoin Is Experiencing Its Longest Stretch Of Price Stability In A While*, BUSINESS INSIDER (Jan. 29, 2014), http://www.businessinsider.com/bitcoin-volatility-slows-2014-1.

50. *Id.*

51. Nakamoto, *supra* note 4, at 1.

52. BRITO & CASTILLO, *supra* note 10, at 4.

53. Fairfield, *supra* note 11, at 14–15.

54. *Id.* at 15.

55. Andreas M. Antonopoulos, *Mastering Bitcoin*, Chapter 1 (2015), http://chimera.labs.oreilly.com/books/1234000001802/index.html.

it is recorded, time-stamped, and cannot be modified.[56] Thus the blockchain accomplishes this task publicly, and requires no third party to verify the transaction.[57] Essentially, *A* transfers ownership of Bitcoin *X* to *B*, and the blockchain records *B* as the new owner of Bitcoin *X*. *A* can no longer double-spend Bitcoin *X* by transferring it to *C* as well since *A* is no longer the owner of that Bitcoin on the public ledger.[58]

There are also a number of other digital currencies, such as Dogecoin, Litecoin, and Darkcoin,[59] but Bitcoin—by name recognition, blockchain hash rate,[60] transaction count, and real world applications—remains by far the most popular.[61]

B. BLOCKCHAIN BASICS: THE MECHANICS OF THE BLOCKCHAIN

The Bitcoin protocol both rewards actors for devoting the processing power of their computers to maintaining the blockchain and makes it prohibitively difficult to falsify a transaction through the mining process.[62]

A useful way to picture the blockchain is as a giant book, with each new block a page added to the top. Each new page contains all the transactions in the network that have been completed since the last page was added. All the Bitcoin miners are competing in a race to solve a complex math problem that will add the next page (block) on top of all the older pages on the public ledger.[63] Whichever miner successfully adds the next page is rewarded in Bitcoins by the Bitcoin protocol.[64]

This analogy is helpful in understanding what makes the blockchain a secure public ledger. For a bad actor to falsify the blockchain, they would have to write all the old pages of the "book" as well as new false counterfeit pages at a speed faster than all the honest users in the network. This task

---

56. Derek A. Dion, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker Cash*, 2013 J.L. TECH. & POL'Y 165, 168 (2013).

57. BRITO & CASTILLO, *supra* note 10, at 4.

58. *See id.*

59. *See Crypto-Currency Market Capitalizations,* COINMARKETCAP, http://coinmarketcap.com/ (last updated Feb. 10, 2015).

60. The number of attempts Bitcoin miners make at solving a particular block of transactions. *See infra* Section I.B.2.

61. *See* Jon Evans, *A Bitcoin Battle Is Brewing*, TECHCRUNCH (Dec. 6, 2014), http://techcrunch.com/2014/12/06/a-bitcoin-battle-is-brewing.

62. ELWELL ET AL., *supra* note 2, at 2.

63. *See* Fairfield, *supra* note11, at 17–21 (describing the process for proving blocks and adding them to the blockchain).

64. *See id.* at 19.

is nearly impossible,[65] and if a major technological breakthrough occurred that allowed a bad actor to marshal hitherto unforeseen amounts of computing power, he or she would be better served by simply applying that power to honest mining.[66] Application of all that computational power to Bitcoin mining would allow that actor to prove blocks at a faster rate than the rest of the network and would create a more predictable source of income.[67] Additionally, a massive hacking of the entire blockchain would cause the value of Bitcoins to plummet, thus making the loot of their crime substantially less valuable.[68] This decentralized mechanism for guaranteeing the security of the system is what makes the blockchain revolutionary. Rather than having a trusted (and hackable[69]) intermediary to verify transactions (such as a bank or credit card company), while imposing large fees for their trouble, the blockchain is a trustless public ledger with substantially lower transaction fees.[70] Put another way, the Bitcoin protocol has created a system that incentivizes good behavior without the need for oversight from a central authority.[71] The resources in terms of sheer computing power required to be a bad

65. Put another way, an attacker would have to guess the hashes enough times to look like the rest of the system, matching the combined processing power of the entire network, and to continue guessing faster than the current block chain. The protocol accepts the block chain with the higher degree of difficulty. Thus an attacker would have to guess more hashes, faster, and at a greater degree of difficulty than the rest of the network. *Id.* at 21.

66. Nakamoto, *supra* note 4, at 4. Notably, two computer scientists at Cornell, Ittay Eyal and Emin Gün Sirer, believe this confidence is misplaced and that the blockchain could be falsified with only a third of miners, as opposed to over half, colluding dishonestly. Eyal and Sirer propose the possibility of a "selfish mining pool" which for reasons based in the Bitcoin Protocol could, with more than one third of miners, severely undermine the system, ultimately destroying its decentralized character. In practice, this would entail a pool of selfish miners working, as honest miners do, on solving a new block to put on top of the blockchain. But instead of publishing that block immediately, the selfish miners would keep the block private. From here, the selfish miners will attempt to build on their lead by finding and solving another block, and just before the honest miners close the gap, the selfish miners would publish their hidden longer chain, nullifying the work of the honest miners. This increase in profits would incentivize more honest miners to join the selfish mining pool and eventually change the blockchain from a decentralized system with all of its benefits of security and finality to a centralized system, operating at the whim of colluding miners. ITTAY EYAL & EMIN GÜN SIRER, MAJORITY IS NOT ENOUGH (2014), *available at* http://www.cs.cornell.edu/~ie53/publications/btcProcArXiv.pdf.

67. *See* Nakamoto, *supra* note 4, at 4.

68. *See id.*

69. *See supra* note 30.

70. ELWELL ET AL, *supra* note 2, at 5.

71. Antonopoulos, *supra* note 55, at Chapter 8.

actor would be more profitably used to support the system rather than undermine it.[72] This is also the process for implementing the monetary supply, which makes the Bitcoin protocol more elegant still.[73]

1. *The Security Features of Bitcoin and the Blockchain*

The Bitcoin protocol is a very secure way to transfer currency because of its utilization of cryptography. Cryptography in the most basic sense is the ability to hide one's communications from people who lack the correct key to decode a communication[74] that might otherwise look like gibberish.[75] Cryptography has been used in one form or another at least since the ancient Greeks,[76] and with the advent of computers and their massive processing power, is the basis for Bitcoin's ability to be transferred securely.[77]

Security in the Bitcoin protocol is ensured through "cryptographic proof," allowing the parties to deal directly with each other, rather than through a third party.[78] Each user's account has two cryptographically related keys, a "public key" and a "private key."[79] The keys are mathematically related, but it is not possible to use the public key to derive the private key.[80] The public key, essentially a string of letters and numbers approximately twenty-seven to thirty-four characters long, is best thought of as an address listed on the blockchain that anyone in the public can see.[81] It acts as the destination at which a user receives Bitcoins.[82]

Only the owner of the Bitcoin knows the "private key", and can use it to authorize or "sign" a transfer of Bitcoins to a different account's[83] public key address. If a malicious actor were to discover another user's private key, that malicious actor would be able to steal that user's Bitcoins.[84]

It is irrelevant how or where the transaction is transmitted to the Bitcoin network as peer-to-peer networks connect each client (also known

72. *Id.*
73. *Id.*
74. *Cryptography Definition*, *supra* note 8.
75. *See* Dion, *supra* note 56, at 168 (a Bitcoin private key is "essentially a string of letters and numbers approximately twenty-seven to thirty-four characters long).
76. V.V. YASHCHENKO, CRYPTOGRAPHY: AN INTRODUCTION 6 (2000).
77. *See* Kaplanov, *supra* note 3, at 116.
78. *Id.*
79. Dion, *supra* note 56, at 167–68.
80. Fairfield, *supra* note 11, at 18.
81. Dion, *supra* note 56, at 168.
82. *Id.*
83. Typically another user, though users can have multiple accounts if they wish.
84. Dion, *supra* note 56, at 184.

as a node) to several other Bitcoin clients.[85] Any Bitcoin node that receives a valid transaction that the node has not seen before will forward the transaction to all connected nodes, and within seconds the transaction will reach a large percentage of nodes.[86]

The public key address contains no information about the user, and though Bitcoin users do enjoy a much higher level of privacy than users of traditional digital-transfer services, staying completely anonymous can be quite difficult.[87] Without knowing to whom a public key address corresponded, in one experiment, researchers found that behavior-based clustering-techniques were able to reveal 40 percent of Bitcoin users.[88] Yet, if a public key were linked to a person's identity, one could look through the recorded transactions on the blockchain and view all transactions associated with that public key.[89] Public key addresses on the public ledger can be identified years after an exchange is made.[90] Once Bitcoin exchanges become fully compliant with bank secrecy regulations requiring firms to collect personal data on their customers this privacy will be further eroded. A more detailed discussion of bank secrecy regulations is below.[91] Anonymity could be guaranteed for a short time if a user were to meet a Bitcoin holder in person and pay that owner for their Bitcoins in cash, but there is evidence that statistical techniques and pattern analysis can unmask up to 60 percent of Bitcoin users.[92]

2. Bitcoin Mining and the Maintenance of the Blockchain

A transaction is not part of the public ledger (blockchain) until verified and included in a block through a process called mining.[93] Mining is both the process for creating Bitcoins and the method for updating the blockchain with the most current transactions.

Transactions are bundled into blocks that are generated every ten minutes in a computationally intense process that requires miners to solve

85. Antonopoulos, *supra* note 55, at Chapter 2.
86. *Id.*
87. BRITO & CASTILLO, *supra* note 10, at 9.
88. Elli Androulaki et al., *Evaluating User Privacy in Bitcoin*, CRYPTOLOGY EPRINT ARCHIVE (2013), https://eprint.iacr.org/2012/596.
89. BRITO & CASTILLO, *supra* note 10, at 8.
90. *Id.* at 9.
91. *See infra* Section IV.B.1.a).
92. ALEX BIRYUKOV ET AL., DEANONYMISATION OF CLIENTS IN BITCOIN P2P NETWORK (2014), *available at* http://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf.
93. *Id.*

a difficult mathematical problem.[94] These problems require a great deal of computation to prove, but very little computation to verify as proven.[95] This "proof-of-work" solution requires quadrillions of computations per second across the entire Bitcoin network.[96] These computations require the computer to guess numbers.[97] Josh Fairfield likens this process to rolling dice.[98] The computation does not in and of itself discover anything, but due to the length of the values to be guessed, it inherently has a mathematically predictable degree of difficulty that can be increased by making the values, or "hashes" longer.[99] The hash is a way of transforming an arbitrary amount of data into a fixed number that is not invertible (the data cannot be deduced from the hash).[100]

Bitcoin mining requires an incredible amount of computing power. In March 2014, an estimated 30,000 trillion hashes per second were computed on the network.[101] Taken as a whole, the Bitcoin network is more powerful than the combined computing power of the top five hundred supercomputers in the world.[102] Security expert Andreas M. Antonopoulos likens Bitcoin mining to a giant game of competitive Sudoku that resets every time a player solves the puzzle. It can take a lot of work to solve the puzzle, but checking the solution is quite simple.[103]

In exchange for proving blocks, miners are rewarded with transaction fees and a set amount of Bitcoins that diminishes as more Bitcoins are mined.[104] The Bitcoin protocol adjusts the difficulty of the computational problems to ensure that Bitcoins mining occurs at a predictable and limited rate;[105] the resulting diminishing returns are meant to simulate the actual diminishing returns that come in real mining.[106] To use Antonpoulos' Sudoku analogy again, the difficulty of the puzzle can be adjusted to require more computing power to solve a block by making the

94. *Id.*
95. *Id.*
96. *Id.*
97. Fairfield, *supra* note 11, at 19.
98. *Id.*
99. *Id.*
100. *Id.* at 20.
101. Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 1, 50 (2014).
102. *Id.* at 50–51.
103. Antonopoulos, *supra* note 55, at Chapter 2.
104. BRITO & CASTILLO, *supra* note 10, 6–7.
105. Antonopoulos, *supra* note 55, at Chapter 2.
106. Like with shovels and dirt and rocks.

puzzle larger (by adding more rows or columns).[107] The protocol sets an arbitrary cap of twenty-one million Bitcoins.[108] 2140 is the predicted date the last "satoshi," or 0.00000001 of Bitcoin will be mined.[109] As this time approaches, miners will incur greater expenses due to the progressively more difficult hashes dictated by the protocol.[110]

Transaction costs will have to rise to allow mining to continue to be profitable.[111] Although transaction fees typically represent 0.5% or less of a Bitcoin miner's income,[112] the rest coming from newly minted Bitcoins, these fees still play an important role as they affect the prioritization of which blocks are processed first, since parties to a transaction can pay higher fees to incentivize miners to solve their block before other blocks.[113] This allows market forces to influence the speed at which a transaction is verified.[114] The minimum transaction fee is currently fixed at 0.0001 Bitcoin, or a tenth of a milli-Bitcoin per kilobyte, but if a user wants their transaction processed more quickly, they can include a higher fee to incentivize miners.[115]

Energy is the primary expense in mining Bitcoins, resulting in the creation of large computer centers in places like Washington State and Iceland, where energy costs are particularly low due to the abundance of hydroelectric and geothermal power.[116] In the early stages of mining, essentially any computer had the processing power to engage in Bitcoin mining, but as the hashes have gotten more difficult, only highly specialized equipment is capable of mining.[117] "Botnets" voluntarily enlist large pools of computers to combine computing power to mine Bitcoins more quickly, while splitting the profits based on the percentage of computing power contributed.[118] There is evidence that hackers have also

---

107. Antonopoulos, *supra* note 55, at Chapter 2.
108. *See* ELWELL ET AL., *supra* note 2, at 2.
109. BRITO & CASTILLO, *supra* note 10, at 7.
110. *Id.*
111. *See id.*
112. Antonopoulos, *supra* note 55, at Chapter 8.
113. *Id.* at Chapter 5.
114. *Id.*
115. Bitcoins are divisible to eight decimal places. The maximum amount of spendable units is more than 2 quadrillion (2000 trillion). *See id.*
116. *See* Nathaniel Popper, *Into the Bitcoin Mines*, N.Y. TIMES (Dec. 21, 2013), http://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/.
117. The specialized equipment used to mine Bitcoins is costly, ranging in price from three to nine thousand dollars. *See* Bitcoin Calculator, BITCOINWISDOM.COM, https://bitcoinwisdom.com/bitcoin/calculator (last visited Jan. 24, 2015).
118. *See, e.g.*, BTC GUILD, https://www.btcguild.com to join (last visited Jan. 24, 2015) ("one of the oldest remaining Bitcoin pools").

conscripted unwitting CPUs to the task.[119] In this scenario, hackers utilize a victim's processor power without their knowledge to mine for Bitcoins, presumably without sharing any profits from proven blocks.[120]

Once a block has been verified through the mining process it is added to the blockchain on top of all the previous blocks before it.[121] Thus, the blockchain essentially contains the history of every Bitcoin from its creation through the present day.[122]

II. POTENTIAL USES OF BITCOIN AND THE BLOCKCHAIN

The potential uses of Bitcoin and the blockchain range from the prosaic, such as lowering both transaction costs and risk of credit card fraud, to the more outré use as a (more) stable currency for residents of countries with volatile currencies, to the revolutionary by creating a new theory of digital property through the blockchain. This Part will first examine the potential benefits from Bitcoin based on its relatively low transaction costs. Then it will examine the goals of the two venture capitalists that have invested the most in Bitcoin and Bitcoin-based companies. Finally, this Part will discuss the creation of a new theory of digital property based on blockchain technology.

A. LOWERED TRANSACTION COSTS

Certain benefits of Bitcoin are fairly intuitive and do not require a substantial rethinking of the digital economy. Bitcoin's ability to lower transaction costs for users is of particular import and is one of its features that is driving its adoption today.

Bitcoin is particularly attractive to small businesses looking for ways to lower their transaction costs. Though credit cards have made transactions much easier for consumers, merchants must pay a variety of authorization fees, transaction fees, statement fees, interchange fees, and customer service fees, to name a few.[123] These fees amount to 2 to 3 percent of the transaction.[124] For a business with a 5 percent profit margin,[125] lowering

119. Dion, *supra* note 56, at 184–85.

120. A victim would have to observe a drop in the performance of their computer, a spike in their electricity bill, or an increased amount of data being sent to and from their computer to realize that their CPU had been enlisted in a botnet.

121. Antonopoulos, *supra* note 55, at Chapter 2.

122. *See* BRITO & CASTILLO, *supra* note 10, at 8.

123. *Id.* at 10–11.

124. CHRIS JAY HOOFNAGLE, JENNIFER M. URBAN & SU LI, BCLT, MOBILE PAYMENTS: CONSUMER BENEFITS & NEW PRIVACY CONCERNS 3 (Apr. 24, 2012).

transaction fees by 1 percent of the businesses' revenue gives an additional 20 percent profit. Additionally, merchants labeled "high risk" by credit card companies who have had difficulty finding payment processors have begun to turn to Bitcoin merchant service providers as an affordable and convenient alternative to credit card companies.[126]

Conducting business through Bitcoin also allows merchants to avoid chargeback fraud, where a consumer reverses payment based on a false claim that the product has not been delivered or a service has not been rendered.[127] The irreversibility of a Bitcoin transaction can prevent this type of fraud, as once a Bitcoin has been transferred on the blockchain, that transfer is irreversible. Traditional credit card services will still allow consumers to enjoy the capability to engage in chargebacks as a protection from unscrupulous merchants or merchant errors.[128] But a merchant may wish to give a discount for payments in Bitcoin to incentivize consumers to forgo their ability to chargeback a credit card transaction, to protect the merchant from potential fraud.

Bitcoin also holds great potential for lowering transaction costs required to send remittances back to relatives in developing countries. Remittances to developing countries were projected to reach $454 billion in 2015.[129] Wire services such as Western Union and MoneyGram charged an average fee of roughly 8 percent for sending remittances in the third quarter of 2014.[130] But with Bitcoin, the transaction fee is less than 0.0005 Bitcoins, or approximately 1 percent, assuming liquidity.[131]

125. The profit margin for restaurants in 2013 was 5.1%. *See* Mary Ellen Biery, *U.S. Restaurants Seeing Fatter Margins*, FORBES (June 22, 2014), http://www.forbes.com/sites/sageworks/2014/06/22/us-restaurants-margins/.

126. "High risk" merchants include jewelry businesses, software sellers, online storage providers, and travel services. These merchants are considered high risk because of their chargeback volume. Bailey Reutzel, *Some Risky Merchants Turn to Bitcoin Processor; Others Go It Alone*, PAYMENTS SOURCE (Nov. 8, 2013), http://www.paymentssource.com /news/some-risky-merchants-turn-to-bitcoin-processor-others-go-it-alone-30159 74-1.html.

127. BRITO & CASTILLO, *supra* note 10, at 12.

128. *Id.* at 12.

129. DILIP RATHA ET AL., MIGRATION AND REMITTANCES: RECENT DEVELOPMENTS AND OUTLOOK SPECIAL TOPIC: FORCED MIGRATION 1 (World Bank, Oct. 6, 2014), *available at* http://siteresources.worldbank.org/INTPROSPECTS/Resources/ 334934128890760745/MigrationandDevelopmentBrief23.pdf.

130. *Id.* at 1, 14 n.13.

131. BRITO & CASTILLO, *supra* note 10, at 14.

Professor Susan Athey, Economics of Technology Professor at the Stanford Graduate School of Business,[132] believes that these benefits would allow the world's unbanked poor to access global markets.[133] Currently, many people in developing countries do not have and are unable to obtain bank accounts, and as a result are completely cut off from international financial markets and participation in the global economy.[134] Even for those with credit cards, many merchants refuse to accept international credit card transactions because the fraud rate is too high.[135] Because the transfer of Bitcoins is instantaneous, merchants can accept the currency without fear of fraud.[136] Additionally, in countries with high inflation, people could use Bitcoin to purchase assets on the global market, like tractors, that better hold their value.[137]

B. BITCOIN AS A STABLE CURRENCY IN WEAK MARKETS AND THE BLOCKCHAIN AS A RECORDING SYSTEM FOR MORE THAN JUST BITCOIN

A number of venture capitalists have begun investing in Bitcoin and blockchain-based businesses.[138] This Section will examine the goals of the two venture capitalists that have invested the most to date, Tim Draper and Marc Andreessen.

Tim Draper,[139] co-founder of the investment firm Draper Fisher Jurvetson,[140] sees the future of Bitcoin in emerging economies.[141] Draper,

---

132. *Susan Athey*, STANFORD GRADUATE SCHOOL OF BUSINESS, http://www.gsb.stanford.edu/faculty-research/faculty/susan-athey (last visited Feb. 26, 2015).

133. Laura Shin, *Who Will Benefit From Digital Currency? Bitcoin Experiment Gives a Glimpse*, FORBES (Nov. 26, 2014), http://www.forbes.com/sites/laurashin/2014/11/26/who-will-benefit-from-digital-currency-bitcoin-experiment-gives-a-glimpse/.

134. *Id.*

135. *Id.*

136. *See id.*

137. *Id.*

138. *See* Nathaniel Popper, *$25 Million in Financing for Coinbase*, N.Y. TIMES (Dec. 12, 2013), http://dealbook.nytimes.com/2013/12/12/venture-capital-bets-big-on-bitcoin/.

139. Draper purchased nearly 30,000 Bitcoins for an estimated $19 million dollars auctioned off by the government from the now-defunct online black market Silk Road. *See* Olga Kharif, *Bitcoin Auction Winner Draper to Big Again in December*, BLOOMBERG (Nov. 18, 2014), http://www.bloomberg.com/news/2014-11-18/bitcoin-auction-winner-draper-to-bid-again-in-december.html. The United States Marshals Service held another sealed bid auction for another 50,000 Bitcoins in December 2014. *See For Sale: 50,000 bitcoins*, U.S. MARSHALS SERV. http://www.usmarshals.gov/assets/2014/dpr-bitcoins/ (last visited Jan. 24, 2015). Draper won 2,000 of the Bitcoins with the remaining balance won by the New York-based

with the help of Bitcoin exchange startup Mirror,[142] seeks to "create new services that can provide liquidity and confidence to markets that have been hamstrung by weak currencies."[143] Financial crises are a constant threat in much of the world, with countries like Argentina serving as instructive examples.[144] From the mid-1970s to 2002, Argentina had eight currency crises, four banking crises, and two sovereign defaults.[145] Graciela Kaminsky has identified ninety-six currency crises between January 1970 and February 2002 in countries across Europe, Asia, and South America.[146] Draper told CNBC's Squawk on the Street television show that he believes that "Bitcoin is a great alternative for . . . economies where inflation really saps the strength of a country's economy" and that he expects "Pagos in Argentina, Pagatech in Africa, and [Coincove in Mexico][147] . . . [to] thrive because people in those countries are not as confident in their own governments' fiat currency."[148] Notably, U.S. dollars already play a strong role in this respect with a vast amount of dollars held abroad as an alternative to local currencies because dollars are a more stable way to preserve wealth.[149] The Federal Reserve estimates that more than two-thirds of $100 bills are held overseas.[150]

---

exchange SecondMarket. Sydney Ember, *At an Auction of Bitcoins Seized From Silk Road, SecondMarket Wins Big*, N.Y. TIMES (Dec. 9, 2014), http://dealbook.nytimes.com/2014/12/09/secondmarket-nearly-sweeps-latest-bitcoin-auction/.

140. DRAPER FISHER JURVETSON, http://dfj.com/teams (last visited Feb. 11, 2015).

141. Sydney Ember, *Winner of Bitcoin Auction, Tim Draper, Plans to Expand Currency's Use*, N.Y. TIMES (July 2, 2014), http://dealbook.nytimes.com/ /07/02/venture-capitalist-tim-draper-wins-bitcoin-auction/,.

142. Mirror is owned by Vaurum. About Mirror, MIRRORX.COM, https://mirrorx.com/#/about (last visited Dec. 22, 2014).

143. Ember, *supra* note 141.

144. Trautman, *supra* note 101, at 67.

145. *Id.* at 68.

146. These countries include Argentina, Bolivia, Brazil, Chile, Columbia, Denmark, Finland, Indonesia, Israel, Malaysia, Mexico, Norway, Peru, Spain, Sweden, the Philippines, Thailand, Turkey, Uruguay, and Venezuela. *Id.* at 66 (citing GRACIELA KAMINSKY, VARIETIES OF CURRENCY CRISES 1 (Nat'l Bureau of Econ. Research, Working Paper No. 10193, 2003), *available at* http://www.nber.org/papers/w10193.pdf).

147. Pagos, Pagatech, and Coincove are mobile payments companies.

148. *Why VC Tim Draper bought all those bitcoins*, CNBC.COM (July 7, 2014), http://www.cnbc.com/id/101816404.

149. *See generally* RUTH JUDSON, CRISIS AND CALM: DEMAND FOR U.S. CURRENCY AT HOME AND ABROAD FROM THE FALL OF THE BERLIN WALL TO 2011 (Bd. of Governors of the Fed. Reserve Sys. Int'l Fin. Discussion Papers, IFDP 1058 Nov. 2012), *available at* http://www.federalreserve.gov/pubs/ifdp/2012/ 1058/ifdp1058.pdf.

150. *Id.* at 12.

Marc Andreessen, co-founder and partner of the venture capital firm Andreessen Horowitz[151] believes that the blockchain's security features are what will allow the technology to flourish.[152] As of March 2014, Andreessen's firm has made approximately $50 million in investments in blockchain related businesses, believed to be more than the investments of any other firm.[153] Andreessen argues that not only will payments in Bitcoin be much safer for consumers than credit cards,[154] but also that the inherent security features of the blockchain will allow for the transfer of digital titles and property.[155] Andreessen suggests that in the future, the blockchain will allow for a trustless transfer, without intermediaries, of digital stocks, equities, bonds, contracts, keys, and titles.[156]

In a similar vein, Jeff Garzik, one of Bitcoin's core developers, has suggested the possibility of "smart" self-executing contracts.[157] For instance, a "smart loan" could automatically adjust interest rates based on the financial performance of the borrower.[158] The contract's code could be written to include automated observation of real world metrics, which now require manual reporting, monitoring, and enforcement.[159] As discretion on the part of the lender is removed, Houman B. Shadab of New York Law School's Center for Business and Financial Law suggests a "smart contract" of this sort would greatly reduce or eliminate the need for litigation, because it removes much of the potential for parties to have a dispute.[160]

---

151. ANDREESSEN HOROWITZ, http://a16z.com/team/ (last visited Feb. 11, 2015).

152. *See* Brian Fung, *Marc Andreessen: In 20 years, we'll talk about Bitcoin like we talk about the Internet today*, WASH. POST (May 21, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/.

153. Gregory Zuckerman, *Web Pioneer Keeps Faith, and Cash, in Bitcoin*, WALL ST. J. (Mar. 21, 2014), http://www.wsj.com/articles/SB10001424052702304026304579453501821936252.

154. Andreessen notes that as Bitcoin transfer is instantaneous when a customer purchases a good with Bitcoins, hackers cannot steal that customer's information during the transfer. While Hackers could still steal Bitcoins from poorly secured merchant computer systems, this does increase the risk of loss, fraud, or identity theft to consumers. *See* Andreessen, *supra* note 43.

155. Fung, *supra* note 152.

156. *Id.*

157. Everett Rosenfeld, *Forget currency, bitcoin's tech is the revolution*, CNBC.COM (Nov. 13, 2014), http://www.cnbc.com/id/102178309#.

158. *Id.*

159. *Id.*

160. *Id.*

C. A NEW THEORY OF DIGITAL PROPERTY MADE POSSIBLE BY THE BLOCKCHAIN

At the outer frontier of theorizing on the impact of the blockchain, Professor Joshua Fairfield of the Washington and Lee University School of Law has proposed that the advent of the blockchain as a trustless public ledger that allows for rivalrous digital property warrants a new theory of property as an information communication and storage system.[161] Fairfield argues that property law has managed the transition to the online ecosystem poorly compared to tort and contract law.[162] Yet, with the advent of the blockchain, true digital ownership interests are now possible and rethinking property as an information protocol will avoid placing false constraints on the extension of traditional property rules to digital assets.[163]

The blockchain can be used to implement a property system by tying real property to specific coins within the chain through tokenization.[164] Tying a legal right to a token is common in property law, with examples ranging from paper deeds for land to paper titles for a car.[165] Thus a Bitcoin, or part of a Bitcoin, could be "tokenized" to represent a real asset, such as land. This "tokenized" coin would not impact the rest of the blockchain, but whoever owned the coin would own its associated commodity, such as a home or automobile.[166] These tokenized coins would have all the aforementioned benefits of any other Bitcoin, such as rivalrousness, security, and would be easily tracked on the decentralized public ledger.[167] A tokenized public ledger would offer new solutions to old property problems, such as low cost secure transfer, easy tracing of transactions, prevention of the double spending problem, and the near impossibility of reversal or falsification.[168]

The vast bulk of owned wealth is recorded in systems that tell users who owns what, and the blockchain can decentralize this information and address what Fairfield calls "one of the great inefficiencies of modern property: its reliance on expensive, inaccurate, hard-to-access, hard-to-search, and insecure ledgers of all stripes."[169] Thus, under a new theory of

161. *See generally* Fairfield, *supra* note 11.
162. *Id.* at 8.
163. *See id.* at 9.
164. *Id.* at 24–26.
165. *Id.* at 25.
166. *Id.* at 24.
167. *See id.* at 26.
168. *Id.*
169. *Id.* at 5.

property as an information protocol, the effectiveness of a property system should be judged on how well it stores and communicates information about ownership.[170] Today property records are contained in a "hodgepodge of relatively inaccurate, sometimes insecure, and often expensive ledgers" that are "notoriously costly to search."[171]

The Mortgage Electronic Registration System ("MERS") is a timely example of a current system that could be improved through public ledger technology. MERS is a database set up by banks to facilitate the transfer of mortgages and track their ownership internally.[172] As of 2007, more than half of all home mortgage loans originated in the United States were registered on the MERS system.[173] MERS is listed as the owner in county land records.[174] Yet New York Attorney General Eric T. Schneiderman alleges that because MERS records are private, MERS has limited the public's ability to track property transfers and thus it is difficult to verify the chain of title for a loan or a current noteholder for many properties.[175] Thus during the foreclosure crisis, it became difficult for borrowers to work out exactly who owned their mortgage and to get help in working out their loans.[176] If all mortgages were recorded on the blockchain, instead of MERS, tracking the chain of ownership and mortgages would be a simple task, and defaulting homeowners could more easily determine which bank has the authority to negotiate refinancing options.

As noted above, the Bitcoin protocol rewards Bitcoin miners in Bitcoins for utilizing their computing power to maintain the blockchain. Thus, for Professor Fairfield's ideas to become a reality, Bitcoins need to be adopted by the broader public.

170. *Id.* at 9.

171. *Id.* at 12.

172. Christopher L. Peterson, *Predatory Structured Finance*, 28 CARDOZO L. REV. 2185, 2211–12 (2007).

173. *Id.* at 2212.

174. *Id.*

175. Chad Bray, *New York Sues Banks Over Mortgage Registry System*, WALL ST. J. (Feb. 3, 2012), http://online.wsj.com/articles/SB1000142405297 0203889904577201060859616158.

176. Gretchen Morgenson, *Mortgage Registry Muddles Foreclosures*, N.Y. TIMES (Sept. 1, 2012), http://www.nytimes.com/2012/09/02/business/fair-game-mortgage-registry-muddles-foreclosures.html.

III. THE DARKER SIDE OF BITCOIN: THE POTENTIAL FOR BLACK MARKETS, THEFT, AND TAX EVASION

Cash remains the ultimate anonymous currency. The U.S. $100 note is particularly popular for laundering the profits of illicit activities.[177] Professor Edgar Feige estimates that U.S. currency is the preferred medium for "facilitating clandestine transactions, and for storing illicit and untaxed wealth."[178] It is estimated that over 50 percent of all hard currency in most countries is used to hide transactions.[179] These illicit transactions include illegal trade in drugs, arms, and sex as well as unreported income to skirt the tax code.[180]

In many ways, Bitcoins and cash share a key property that makes them both suitable for unlawful activity: neither requires an institutional (and subpoenable) intermediary.[181] In the same way that it can be hard to track the movements of a briefcase full of $100 bills in a direct transaction between two parties, it can be difficult to track a direct exchange of Bitcoins between two parties.[182] Like cash, there is nothing inherently nefarious about Bitcoins, but the digital nature of Bitcoin introduces a new wrinkle as it can be sent electronically, rather than requiring a physical meeting to exchange.

In the popular imagination, Bitcoin is associated with online black markets, unsavory characters, and risks to consumers from hackers.[183] This view is not entirely unwarranted. Bitcoin has been used as a key

---

177. *See* Chris Arnold, *Should We Kill the $100 Bill?*, NPR'S PLANET MONEY (Aug. 14, 2014), http://www.npr.org/blogs/money/2014/08/14/340356790/should-we-kill-the-100-bill.

178. Edgar L. Feige, *New Estimates of U.S. Currency Abroad, the Domestic Money Supply and the Unreported Economy* 4 (Munich Personal RePEc Archive, Working Paper No. 34778, 2011), *available at* http://mpra.ub.uni-muenchen.de/34778/1/MPRA_paper_34778.pdf.

179. Kenneth Rogoff, *Costs and benefits to phasing out paper currency*, Presentation at NBER Macroeconomics Conference (April 11, 2014), *available at* http://scholar.harvard.edu/files/rogoff/files/c13431.pdf.

180. Feige, *supra* note 178, at 4.

181. A hand-to-hand cash transaction lacks an institutional middleman. Similarly there is no Bitcoin company to raid or shut down in a direct transfer. *See* Kaplanov, *supra* note 3, at 168.

182. *See* BRITO & CASTILLO, *supra* note 10, at 7–8.

183. Stephen T. Middlebrook & Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813, 818–19 (2014).

component of illegal mail order drug and firearm markets,[184] in Ponzi schemes to defraud investors,[185] and has been stolen in large quantities by hackers.[186] Protecting society from these unlawful uses and vulnerabilities is vital to Bitcoin's wider adoption by the general public, and perhaps especially with older users.[187]

This Part will examine the most famous Bitcoin black market website, the disbanded "Silk Road" and its successor Agora, as examples of unlawful activities facilitated by the use of Bitcoin. Next, it will examine the hacked Bitcoin exchange Mt. Gox where consumers lost millions of dollars, as an example of the risks to consumers from improperly secured Bitcoin exchanges. Finally, it will explore Bitcoin's potential use for tax evasion.

A. ONLINE BLACK MARKETS: THE SILK ROAD

Silk Road was a deep Web[188] black-market site in operation from February 2011 to October 2013.[189] Through the anonymizing network TOR,[190] the pseudonymous nature of Bitcoin, plus "tumbling" services such as Bitcoin Bath,[191] users could order drugs and other illicit wares by mail.[192] It is estimated that while operational, Silk Road's transactions

184. *See* Jerry Brito, *Online Cash Bitcoin Could Challenge Government, Banks,* TIME TECHLAND, (Apr. 16, 2011), http://techland.time.com/2011/04/16/online-cash-bitcoin-could-challenge-governments/2/.

185. *See infra* Section IV.C.1; Secs. & Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2014 WL 4652121 at *8 (E.D. Tex. Sept. 18, 2014) (finding defendants' operation to be a "sham and a Ponzi scheme").

186. BRITO & CASTILLO, *supra* note 10, at 22.

187. In a recent survey, of Americans aware of Bitcoin, people over the age of 55 were significantly less likely to choose to invest in Bitcoin rather than gold. Melanie Flanigan, *Most Americans Still Don't Trust Bitcoin Despite Widespread Awareness, New Survey Shows,* YODLEE, (Mar. 25, 2014), http://ir.yodlee.com/releasedetail.cfm?releaseid=867331.

188. The "deep Web" refers websites on the internet that are not accessible through search engines. *See* Michael K. Bergman, *The Deep Web: Surfacing Hidden Value*, 7 J. OF ELEC. PUBL'G 1 (Aug. 2001).

189. *See* BRITO & CASTILLO, *supra* note 10, at 23.

190. The Onion Router or TOR is software that allows users to browse the Internet in complete anonymity and free from third-party tracking by constantly changing the Internet Protocol ("IP") address of a computer. With TOR, users can explore the "deepnet" and explore sites that only host anonymous users. Dion, *supra* note 56, at 166.

191. A tumbling service combines payments from multiple buyers to multiple sellers to obscure which public keys were involved in a transaction. *See What do we do*?, BITCOINBATH, http://bitcoinbath.com/ (last visited Nov. 18, 2014).

192. *See* BRITO & CASTILLO, *supra* note 10, at 23.

amounted to $1.2 million monthly, representing only 0.15% of the $770 million in Bitcoin transactions in a single month.[193]

On October 1, 2013, Federal Bureau of Investigation ("FBI") agents and federal prosecutors in New York apprehended the Silk Road's mastermind Ross Ulbricht, also known as the Dread Pirate Roberts, in a San Francisco library with his laptop open.[194] This action allowed the FBI to shut down Silk Road and seize nearly 30,000 Bitcoins.[195]

Agora, the "online bazaar for contraband," has most successfully replaced Silk Road.[196] Silk Road 2.0 was also launched in November 2013 by several of the administrators from the original Silk Road (and shut down by federal authorities in November 2014).[197] Agora's 16,137 products for sale as of September 2014 is about two hundred more listings than Silk Road 2.0 posted, and several thousand more listings than offered on the original Silk Road.[198] These listings include the perfunctory cornucopia of drugs, but unlike the original Silk Road, also include semi-automatic firearms.[199] Like the Silk Road, business on Agora is conducted in Bitcoins.[200]

B. MT. GOX AND THE RISKS OF INADEQUATE DATA SECURITY TO CONSUMERS

Another key risk to Bitcoin users is having their Bitcoins stolen by hackers due to inadequate security by Bitcoin exchanges and other

193. *Id.* at 24.

194. David Segal, *Eagle Scout. Idealist. Drug Trafficker?*, N.Y. TIMES (Jan. 18, 2014), http://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html.

195. Rachel Abrams & Sydney Ember, *U.S Prepares for Sale of Bitcoins Seized in Its Raid on Silk Road*, N.Y. TIMES (Jan. 18, 2014), http://dealbook.nytimes.com/2014/06/26/u-s-prepares-for-sale-of-bitcoins-seized-in-silk-road-raid/. These were the Bitcoins ultimately purchased by Tim Draper for use by the company Vaurum. *See supra* Section II.B.

196. *See* Andy Greenberg, *Drug Market 'Agora' Replaces the Silk Road as King of the Dark Net*, WIRED (Sept. 2, 2014), http://www.wired.com/2014/09/agora-bigger-than-silk-road/; There are a number of other online black markets with similar, but fewer, offerings. *See Darknet Marketplace Watch – Monitoring Sales of Illegal Drugs on the Darknet*, DIGITAL CITIZENS ALLIANCE, http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=Darknet (last visited Sept. 2, 2014).

197. *See Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court*, FEDERAL BUREAU OF INVESTIGATION (Nov. 6, 2014), http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court.

198. Greenberg, *supra* note 196.

199. *Id.*

200. *Id.*

Bitcoin-based businesses. Bitcoin-based companies and exchanges are inherently new businesses due to the recent development of the Bitcoin protocol.[201] As a result, these companies may not have the resources to fend off hackers that larger and more established institutions might.

Mt. Gox, one of the oldest Bitcoin exchanges, serves as a cautionary tale. Mt. Gox, founded in 2009 as an exchange for Magic: The Gathering cards[202] eventually became the dominant online marketplace for the purchase and sale of Bitcoins, handling 80 percent of all Bitcoin trading activity in 2013.[203] On February 25, 2014, Mt. Gox failed after hackers stole approximately 850,000 Bitcoins.[204] Mt. Gox was eventually able to recover roughly 200,000 of the stolen Bitcoins.[205] This was not the first time hackers had attacked Mt. Gox.[206] In 2011 a hacker stole $8.75 million at the contemporaneous exchange rate.[207] Mt. Gox's failure stands as a cautionary tale, not against the security of the blockchain itself, but rather against the security of the intermediaries who are not subject to the same capital holdings requirements as regular banks and stock exchanges.

C. BITCOIN AS A VEHICLE FOR TAX EVASION

Omri Marian, Assistant Professor of Law at the University of Florida Levin College of Law, proposes that cryptocurrencies such as Bitcoin will become key vehicles for tax evasion.[208] Marian believes two factors suggest that tax evaders, who have traditionally evaded taxes through offshore bank accounts in tax-haven jurisdictions, will instead use cryptocurrencies to facilitate their evasion.[209] The first factor is the increasing popularity of cryptocurrencies such as Bitcoin that function with their own free-floating

201. "The first Bitcoin specification and proof of concept was published in 2009." *Frequently asked questions*, BITCOIN.ORG, https://bitcoin.org/en/faq (last visited Feb. 11, 2015).

202. "Magic is a tradable card game (TCG) where you build your collection of cards by trading with your friends, assembling decks of cards, and battling against an opponent and their deck." *See What is Magic: The Gathering*, http://magic.wizards.com/en/what-is-magic (last visited Nov. 18, 2014). This author was particularly fond of the game between 1998–2001.

203. Trautman, *supra* note 101, at 100–01.

204. Takashi Mochizuki & Eleanor Warnock, *Mt. Gox Head Believes No More Bitcoins Will Be Found*, WALL ST. J. (June 29, 2014), http://online.wsj.com/articles/mt-gox-head-believes-no-more-bitcoin-will-be-found-1403850830.

205. *Id.*

206. *See* Dion, *supra* note 56, at 185.

207. *Id.*

208. Omri Y. Marian, *Are Cryptocurrencies Super Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38, 39 (2013).

209. *Id.*

exchanges. Second, many governments' preferred anti-tax evasion strategy has changed from targeting tax havens that host financial intermediaries to the financial intermediaries themselves.[210]

Since the 2010 enactment of the Foreign Accounts Tax Compliance Act ("FATCA"), foreign financial institutions ("FFIs") are required to identify their U.S. account holders to the Internal Revenue Service ("IRS"), or face a 30 percent gross tax on payments received from U.S. sources.[211] This gives FFIs with substantial business in the United States the choice of either breaching their home jurisdiction's bank secrecy laws or paying a heavy tax in the United States.[212] But FATCA was enacted and negotiated with multiple intergovernmental agreements requiring foreign governments to relax their own bank secrecy laws or risk losing business with U.S. firms, thus FFIs in many jurisdictions can comply with FATCA without breaching their local bank secrecy laws.[213]

Cryptocurrencies possess a number of important advantages over traditional tax havens. First, as Bitcoins can be held in online wallets, they do not operate in a particular jurisdiction like a traditional tax haven and are not subject to taxation at the source.[214] Second, they are pseudonymous[215] and users can have as many wallets as they wish, potentially without providing any identifying information.[216] Third and most important, Bitcoin and other cryptocurrencies are not dependent on financial intermediaries such as banks.[217] Ordinarily, the IRS may compel financial institutions to produce records to be used in an investigation or trial.[218] But with Bitcoin, these financial institutions are absent and investigators would have to compel the parties to the transaction to admit their involvement.[219] Thus, Marian argues, the IRS would not have an FFI to target, and Bitcoin wallets would skirt international anti-evasion laws

210. *Id.*

211. *Id.* at 40–41.

212. *Id.* at 41.

213. *Id.*

214. *Id.* at 42.

215. *See id.; supra* Section I.B.1. Marian argues Bitcoin public key accounts are anonymous, though this Note has established that in fact these public key addresses are pseudonymous. Still, if an account holder simply made deposits in to a Bitcoin wallet and never made withdrawals, statistical analysis techniques for unmasking users would be less useful.

216. *Id.*

217. *Id.*

218. *Id.* at 41.

219. *Id.* at 42.

such as FATCA, unless they self-reported.[220] This is something a tax evader is certain not to do.

Though current U.S. bank secrecy laws[221] applied to Bitcoin exchanges could obviate this problem, more sophisticated approaches to evasion might still succeed.[222] For instance, an evader, through tax-exempt buying agents, could invest in traded securities and commodities using a Bitcoin-equity swap contract.[223] In this scenario the evader would pay the agent in Bitcoin the amount she wants to invest in a stock.[224] The agent would purchase the stock using the dollar value of the Bitcoin paid, and transfer any dividends back to the evader. As the agent is tax-exempt, he would carry no tax liability.[225] Thus tax authorities would know nothing about the involvement of the Bitcoin investor, whose income from investment would go unreported and untaxed.[226] Though this may sound convoluted, tax evasion is estimated to cost the United States between $40 to $70 billion in tax revenues each year, and is thus quite profitable to evaders.[227]

IV. ANALYSIS OF APPLICABLE LAWS, REGULATION BY GOVERNMENT AGENCIES, AND TREATMENT IN THE COURTS

This Part will describe the current regulatory landscape around Bitcoin by government agencies and how U.S. courts have dealt with cases involving Bitcoin. The first Section will examine relevant laws that may be, or are being, used to regulate Bitcoin. The second Section will examine the regulation of Bitcoin by federal agencies. The final Section will argue that U.S. courts have treated Bitcoin from a functional perspective that is best described as "you did an unlawful thing, and you are not excused because that unlawful thing was done with Bitcoin."

Statutes and regulations around Bitcoin fall into two broad categories: those that protect people who use Bitcoins (consumers, investors), and those that protect society from people who use, or might use, Bitcoins (drug dealers, terrorists, violent criminals). The first category consists of

220. *See id.* at 42.
221. This is discussed below *infra* at Section IV.A.3.
222. Marian, *supra* note 208, at 42–43.
223. *Id.*
224. *Id.* at 43.
225. *Id.*
226. *Id.*
227. *See id.* at 40 (citing JANE G. GRAVELLE, CONGRESSIONAL RESEARCH SERVICE, R40623, TAX HAVENS: INTERNATIONAL TAX AVOIDANCE AND EVASION 1 (2013)).

statutes and regulations that protect Bitcoin users from fraud and theft. The second category consists of statutes and regulations to protect society from the "Four Horsemen of the Infocalypse."[228] Notably, many of the enforcement mechanisms are directed at Bitcoin exchanges.[229] Like cash, Bitcoins sent directly to another person without an intermediary are more difficult to track than electronic transactions involving credit cards.[230] Thus, for regulators Bitcoin exchanges are the most logical institutional choke point in the Bitcoin ecosystem.

A. APPLICABLE LAWS

1. *The Stamp Payments Act*

As a threshold matter, it does not appear that the U.S. government is seeking to outlaw Bitcoins completely.[231] But if the government were to attempt this, many commentators believe the Stamp Payments Act of 1862 ("Stamp Payments Act") might be a potential mechanism.[232] The Stamp Payments Act was enacted when inflation caused the metal in low denomination coins to be more valuable than the face value of the coins themselves, causing people to hoard the coins and creating a shortage.[233] In order to make change for customers in the absence of these coins, companies privately issued small denominations of currencies in notes or tokens.[234] Economists and politicians feared that these private currencies were contributing to inflation and enacted the Stamp Payments Act,[235] which in relevant part states:

228. A term coined at the dawn of the information age to describe the four key threats of the information age: drugs, money laundering, child pornography, and terrorism. The Four Horsemen are used as justification for many cyber security policies and practices. Bruce Sterling, *The Cybersecurity Industrial Complex*, WIRED (Jan. 2003), http://archive.wired.com/wired/archive/11.01/view.html?pg=4.

229. *Infra* Section IV.B.1.a).

230. *See* ELWELL ET AL, *supra* note 2, at 2–3.

231. Though Senator Joe Manchin of West Virginia has called for as much. *See Manchin Demands Federal Regulators Ban Bitcoin*, JOE MANCHIN NEWSROOM (Feb. 26, 2014), http://www.manchin.senate.gov/public/index.cfm/2014/2/manchin-demands-federal-regulators-ban-bitcoin.

232. *See, e.g.*, Dion, *supra* note 56, at 174–75; Grinberg, *supra* note 6, at 186; *but see* Matthew Kien-Meng Ly, *Coining Bitcoin's "Legal Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J. L. & TECH. 587, 598–99 (2014).

233. Grinberg, *supra* note 6, at 183.

234. *Id.*

235. *Id.*

> Whoever makes, issues, circulates, or pays out any note, check, memorandum, token, or other obligation for a less sum than $1, intended to circulate as money or to be received or used in lieu of lawful money of the United States, shall be fined under this title or imprisoned not more than six months, or both.[236]

Though this might appear to apply to Bitcoins, which are divisible into sums of less than one dollar, caselaw suggests that the touchstone of the Stamp Payments Act is competition with official currency.[237] Grinberg suggests that the following factors in determining whether a note or token is in competition with official currency can be derived from caselaw. Grinberg posits that the Stamp Payments Act "is unlikely to apply to anything that (1) circulates in a limited area, (2) is redeemable only in goods, (3) does not resemble official U.S. currency and is otherwise unlikely to compete with small denominations of U.S. currency, or (4) is a commercial check."[238] Though Bitcoin arguably is intended to compete with official currency, banning Bitcoin under the Stamp Payments Act would not further Congress's goal of preventing competition with U.S. coins.[239] Additionally, as the Stamp Payments Act provides criminal penalties, a court might narrowly interpret it to conclude that Congress did not anticipate Bitcoin and it is thus not within the scope of the Stamp Payments Act.[240] There have been no published court opinions interpreting the Stamp Payments Act since 1899 and it is unlikely it will be revived to outlaw Bitcoin.[241]

2. The Securities Act

The use of Bitcoin as an investment tool has brought it to the attention of the Securities and Exchange Commission ("SEC"), under the ambit of the Securities Act of 1933.[242] The Securities Act of 1933 ("Securities Act") defines securities in broad terms through a thorough list of financial instruments.[243] Courts have painted the scope of the Securities

236. 18 U.S.C. § 336 (2012).

237. *See* Grinberg, *supra* note 6, at 183–84 (citing Stettinius v. United States, 5 D.C. (5 Cranch) 573 (D.C. Cir. 1839); United States v. Monongahela Bridge Co., 26 F. Cas. 1292, 1292 (W.D. Pa. 1863) (No. 15,796)).

238. Grinberg, *supra* note 6, at 185 (citations omitted).

239. *Id.* at 187.

240. *Id.*

241. *Id.* at 190–91.

242. *See* Secs. & Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2014 WL 4652121 (E.D. Tex. Sept. 18, 2014); *infra* Section IV.A.2.

243. *See* 15 U.S.C. § 77(b) (2012).

Act with a broad brush[244] and, as discussed below, have already ruled that investment schemes involving Bitcoin qualifies.[245]

Commentator Paul H. Farmer Jr. argues that Bitcoin itself could be considered a security or an investment contract, as many purchasers of Bitcoin buy the digital currency simply to speculate on its value, rather than to use it for the purchase of goods and services.[246] Yet, the SEC has not categorized the purchase of Bitcoins as buying a security or investment contract. Instead the agency has pursued people for operating Ponzi schemes[247] and selling unregistered securities[248] involving Bitcoin, not for the simple purchase of Bitcoin itself. In both these actions, the SEC was not saying that the purchase of a Bitcoin on an exchange counted as a security or investment contract, rather that schemes that involved Bitcoin in lieu of dollars were not exempt from the SEC's enforcement authority.

Commentator Derek A. Dion has argued that regulating Bitcoin exchanges under the SEC might be both logical and desirable.[249] Under this conception, Bitcoin exchanges bring together willing buyers and sellers on a virtual trading floor to, as Dion suggests, seek a future return based on the action of others.[250] Should the SEC regulate exchanges, the exchanges would have to register with the agency, file public reports (which would provide better information to purchasers and the government) and be liable for instances of fraud.[251] While these consumer protection benefits are desirable, they are inconsistent with how the SEC has chosen to frame Bitcoin: as a currency to purchase a security or investment contract, but not as the security or investment contract itself.

---

244. Reves v. Ernst & Young, 494 U.S. 56, 60 (1990) ("In defining the scope of the market that it wished to regulate [through the Securities Acts], Congress painted with a broad brush.").

245. *See Shavers*, 2014 WL 4652121 at *12; *infra* Section IV.C.1.

246. Paul H. Farmer Jr., *Speculative Tech: The Bitcoin Legal Quagmire & the Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85, 98–104 (2014).

247. *See, e.g.*, *SEC Charges Texas Man With Running Bitcoin-Denominated Ponzi Scheme*, SECS. & EXCH. COMM'N NEWSROOM (July 23, 2013), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583#.VGzeTZPF9aQ.

248. *See, e.g.*, *SEC Charges Bitcoin Entrepreneur With Offering Unregistered Securities*, SECS. & EXCH. COMM'N NEWSROOM (June 3, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541972520#.VGzeMJPF9aQ.

249. *See* Dion, *supra* note 56, at 193–94.

250. *Id.* at 193.

251. *Id.* at 194.

3. *The Electronic Funds Transfer Act*

The Electronic Funds Transfer Act of 1978 ("EFTA"),[252] along with the Federal Reserve's Regulation E,[253] were enacted to establish the "rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems" and primarily the "provision of individual consumer rights."[254] The EFTA regulates financial institutions that both hold accounts belonging to customers and perform electronic funds transfers,[255] and requires those institutions to take consumer protection measures such as reversal rights on transactions.[256]

The Bitcoin system itself does not qualify as a financial institution, as it is a decentralized program on which users may transact with each other directly.[257] Yet, Bitcoin exchanges may fall under the purview of the EFTA.[258] Imposing chargeback requirements on Bitcoin exchanges is incompatible with one of the key features and advantages of the blockchain—its irreversibility.[259] Professor Fairfield suggests that a flexible construction of the chargeback requirement through an escrow system might be enough to satisfy regulators.[260] Although such a system would not allow for formal chargebacks, an escrow system that withholds funds for a grace period would continue to serve the same consumer protection function.[261]

B. BITCOIN AND FEDERAL AGENCIES

1. *Regulations to Combat the Four Horsemen: "Protecting Us From Bitcoin Users"*

This Section will examine how federal agencies have enforced regulations to combat the use of Bitcoin to facilitate unlawful activities. First, it will examine the Financial Crimes Enforcement Network's ("FinCEN") regulation of Bitcoin exchanges under the Bank Secrecy Act ("BSA") to preventmoney laundering. Second, it will examine how the

252. 15 U.S.C. §§ 1601–1693 (2012).
253. 12 C.F.R. 205.1–205.20 (2012).
254. 15 U.S.C. § 1693(b).
255. 12 C.F.R. 205.1(b).
256. Reversal rights for credit card holders stem from Regulation Z of the Truth in Lending Act 12 C.F.R. §§ 226.1–226.59. Reversal rights for debit card holders come from Regulation E of the Electronic Fund Transfer Act, *supra* note 253.
257. Ly, *supra* note 1, at 599; BRITO & CASTILLO, *supra* note 10, at 36.
258. BRITO & CASTILLO, *supra* note 10, at 35–38.
259. *Id.* at 37–38.
260. *See* Fairfield, *supra* note 11, at 41–42.
261. *Id.* at 42.

FBI auctioned off some of the Bitcoins seized from the operation to shut down the Silk Road.

a) FinCEN

On March 18, 2013, the FinCEN issued guidance clarifying that certain businesses or individuals who use or make a business of exchanging, accepting, and transmitting virtual currencies were subject to the requirements of the BSA.[262] FinCEN is a bureau housed within the U.S. Department of the Treasury, in charge of enforcing the BSA, a comprehensive anti-money laundering and counter-terrorism financing statute.[263] FinCEN later amended the ruling to exempt Bitcoin miners and companies purchasing and selling virtual currency as an investment exclusively for the company's benefit from the BSA.[264]

Recently, in response to an unnamed company's actions, FinCEN ruled that Bitcoin exchanges which operate only to match sellers and buyers also qualify as money transmitters.[265] Some observers believe this administrative ruling might expand the reach of FinCEN registration requirements to Bitcoin processors which route Bitcoin from customers to merchants, creating reporting and compliance standards on essentially any company that transfers Bitcoin in commerce.[266]

As with the IRS ruling below, FinCEN's decision helps solidify the legal responsibilities associated with virtual currency, and imposes registration, reporting, and recordkeeping burdens on certain businesses. As Bitcoin and virtual currency are still in the nascent stages of their development, these requirements may be prohibitively difficult for emerging companies to adhere to. A potential solution that would allow Bitcoin startups to build enough capital to succeed while remaining

262. *FinCEN Issues Guidance on Virtual Currencies and Regulator Responsibilities*, FIN. CRIMES ENFORCEMENT NETWORK (Mar. 18, 2013), http://www.fincen.gov/news_room/nr/pdf/20130318.pdf.

263. *See What We Do*, FIN. CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/about_fincen/wwd/ (last visited Jan. 25, 2015).

264. *FinCEN Publishes Two Rulings on Virtual Currency Miners and Investors*, FIN. CRIMES ENFORCEMENT NETWORK (Jan. 30, 2014), http://www.fincen.gov/news_room/nr/pdf/20140130.pdf.

265. JAMAL EL-HINDI, FIN. CRIMES ENFORCEMENT NETWORK, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL CURRENCY PAYMENT SYSTEM 1 (Oct. 27, 2014), *available at* http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf.

266. *See, e.g.*, Pete Rizzo, *FinCEN Rules Bitcoin Payment Processors, Exchanges are Money Transmitters*, COINDESK (Oct. 27, 2014), http://www.coindesk.com/fincen-rules-bitcoin-payment-processors-exchanges-money-transmitters/.

compliant with FinCEN regulation might include exempting Bitcoin exchanges from state regulation and setting a revenue amount at which point registration is required.

b) The Federal Bureau of Investigation

In 2013, the FBI shut down Silk Road, a website that acted as a virtual black market and operated using solely Bitcoins to purchase drugs, forged documents, and even possibly assassins for hire.[267] In a dramatic arrest in the San Francisco Public Library, the Silk Road's alleged mastermind Ross Ulbricht (known online as the Dread Pirate Roberts) was captured with his laptop open.[268] Ulbricht's laptop was purportedly a hub of more than $1.2 billion worth of transactions in illicit substances and key to the FBI seizure of Ulbricht's own personal stash of Bitcoins, valued at the time at $80 million.[269]

The federal government has a responsibility to sell property seized from criminals,[270] and selling the Bitcoins at maximum value represented a unique challenge.[271] The seized Bitcoins represented a substantial percentage of the average daily trading volume of Bitcoins, and the FBI feared that dumping them all on the virtual exchanges would flood the market and depress values.[272] To prevent this, the FBI sold the Bitcoins as

267. *See* Joseph Goldstein, *Arrest in U.S. Shuts Down a Black Market for Narcotics*, N.Y. TIMES (Oct. 2, 2013), http://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html.

268. Segal, *supra* note 194.

269. United States v. Ulbricht, 2014 WL 901601 (S.D.N.Y. Feb. 4, 2014); Segal, *supra* note_194, (Ulbricht's computer was the command center of Silk Road); *see* infra Section IV, Part B.

270. *See* *Asset Forfeiture*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/investigate/white_collar/asset-forfeiture (last visited Jan. 25, 2015).

271. *See* U.S. v. Ulbricht No. 13 Civ. 6919 (S.D.N.Y. 2014) (noting that the U.S. and Ulbricht agree that "due to the volatile market for bitcoins, the . . . Bitcoins risk losing value during the pendency of the forfeiture proceedings").

272. *See* Sydney Ember, *Another Bitcoin Auction to Be Held by U.S. Marshalls*, N.Y. TIMES (Nov. 17, 2014), http://dealbook.nytimes.com/2014/11/17/another-bitcoin-auction-to-be-held-by-u-s-marshals/.

property in a secret auction[273] with venture capitalist Tim Draper winning all 30,000 Bitcoins at issue.[274]

2. *Regulations Designed for Consumer Protection: "Protecting Bitcoin Users"*

The other category of government agency oversight of Bitcoins and the blockchain is focused on consumer protection. Whereas the previous Section concerned agency action to protect society from unlawful uses of Bitcoin, this Section will examine how a number of federal agencies are seeking to prevent Bitcoin users from being defrauded, manipulated, and robbed.

First this Section will examine the IRS's classification of Bitcoin as property, not currency. This is a problematic classification for the wider adoption of Bitcoin as a currency. Next it will examine the efforts of the Commodities Futures Trading Commission and Consumer Financial Protection Bureau to ensure the safety of Bitcoin related products and services to consumers. Finally it will examine the New York Department of Financial Services proposed licensing regime for companies that hold Bitcoins for customers.

a) The IRS's Classification of Bitcoin as Property is an Obstacle to the Widespread Adoption of Bitcoin as a Currency

On March 25, 2014 the IRS issued a notice stating that for federal tax purposes, the IRS would treat virtual currency as property, rather than currency.[275] The IRS will apply general tax and reporting principles that govern property transactions to those transactions involving virtual currencies such as Bitcoin.[276] This ruling is the government regulation most inapposite to the widespread adoption of Bitcoin as a currency.

---

273. The FBI arranged for an online auction for the 30,000 seized Bitcoins in a 12-hour window to submit a single sealed bid for coins broken up into lots of 3,000. The FBI was concerned with Bitcion's potential to be used for illegal activity and the agency screened potential bidders, who had to prove their identities and have at least $200,000 in cash. The FBI partially botched the sale by accidentally releasing the list of bidders. *See* Abrams & Ember, *supra* note 195.

274. Pete Rizzo, *VC Tim Draper Revealed as Silk Road Bitcoin Auction Winner*, COINDESK (July 2, 2014), http://www.coindesk.com/tim-draper-revealed-silk-road-bitcoin-auction-winner/.

275. *IRS Virtual Currency Guidance: Virtual Currency is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*, INTERNAL REVENUE SERVICE (Mar. 25, 2014), http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance.

276. *Id.*

The IRS's ruling also means that Bitcoin investors are considered stock investors, and able to take advantage of lower capital gains taxes, and certain tax write-offs, unavailable with regular property.[277] Some have praised the IRS's decision as bringing certainty to the public.[278]

Treating Bitcoin as property has profound implications for Bitcoin transactions as it creates new income tax liabilities.[279] For instance, if an individual acquired a Bitcoin for one dollar and subsequently used it to purchase a three-dollar cup of coffee, this transaction would trigger two dollars in capital gains for the purchaser of coffee (because his original investment was one dollar) and three dollars of gross income for the coffee seller.[280] Simply tracking this sort of information might be prohibitively difficult or tedious. Some commentators, such as Pamir Gelenbe, a venture partner with Hummingbird Ventures, believes this will depress adoption of Bitcoin as it requires considering capital gains when using Bitcoins to make purchases.[281] If the goal is to promote the widespread adoption of Bitcoin as a currency among the general public, the IRS's decision to treat it as property is counterproductive.

Others believe this fear is overblown. Attorney Greg Broiles, a specialist in estate planning, trust, and probate, argues only significant purchases would require these decisions.[282] For instance, it might matter if purchasing a motorcycle, but not matter if purchasing a sandwich.[283] In early 2014, Overstock.com's average order size for customers paying in Bitcoin was $226, 34 percent higher than customers paying in dollars.[284] This suggests that many people using Bitcoins to purchase goods are making purchases in between the ham sandwich and motorcycle range. Data is unavailable as to how many of these purchasers declared, or plan to declare, capital gains.

---

277. *See* Richard Rubin & Carter Dougherty, *Bitcoin Is Property, Not Currency, In Tax System: IRS*, BLOOMBERG.COM (Mar. 25, 2014), http://www.bloomberg.com/news/2014-03-25/bitcoin-is-property-not-currency-in-tax-system-irs-says.html.

278. *Id.*

279. *Id.*

280. *Id.*

281. *Id.*

282. Danny Bradbury, *What the IRS Bitcoin Tax Guidelines Mean For You*, COINDESK (Mar. 26, 2014), http://www.coindesk.com/irs-bitcoin-tax-guidelines-mean/.

283. *Id.*

284. Patrick Byrne, *Coinbase and Overstock.com: The Results are In!*, COINBASE BLOG (Mar. 4, 2014), http://blog.coinbase.com/post/78558321110/coinbase-and-overstock-com-the-results-are-in.

b) Commodity Futures Trading Commission

The Commodity Futures Trading Commission ("CFTC") regulates commodities futures, the markets those futures are traded on, and certain foreign exchange instruments under the Commodity Exchange Act.[285] The mission of the CFTC is to "to avoid systemic risk, and to protect the market users and their funds from fraud, manipulation, and abusive practices related to derivatives and other products that are subject to the Commodity Exchange Act."[286]

Recently, CFTC Commissioner Mark P. Wetjen stated that he believed the CFTC had the authority to regulate price manipulation in Bitcoin markets.[287] Commissioner Wetjen stated that the CFTC had this authority "because if you think of any reasonable reading of our statute, [B]itcoin classifies as a commodity."[288] To wit, the CFTC has also made the first approval of a Bitcoin derivatives trade by the firm TeraExchange.[289]

c) Consumer Financial Protection Bureau

The newly established Consumer Financial Protection Bureau's ("CFPB") mission is to "make markets for consumer financial products and services work for Americans."[290] Although the CFPB has not taken any direct action to regulate Bitcoin yet, in August 2014 the CFPB issued a consumer advisory statement warning the public of the risk of Bitcoins.[291] The advisory warned consumers about potential hackers, that Bitcoin offered fewer protections as compared to banks or debit and credit card providers, and had potentially higher costs and scams.[292] The CFPB

285. 7 U.S.C. §§ 1–27.

286. *Mission & Responsibilities*, U.S. COMMODITIES FUTURE TRADING COMM'N, http://www.cftc.gov/About/MissionResponsibilities/index.htm (last visited Nov. 29, 2014).

287. Michael J. Casey, *CFTC Commissioner Says Agency Has Authority Over Bitcoin Price Manipulation*, WALL ST. J. (Nov. 17, 2014), http://online.wsj.com/articles/cftc-commissioner-says-agency-has-authority-over-bitcoin-price-manipulation-1416265016.

288. *Id.*

289. *TeraExchange Completes First Bitcoin Derivatives Trade on Regulated Exchange*, PR NEWSWIRE (Oct. 9, 2014), http://www.prnewswire.com/news-releases/teraexchange-completes-first-bitcoin-derivatives-trade-on-regulated-exchange-278661591.html.

290. *About Us*, CFPB, http://www.consumerfinance.gov/the-bureau/ (last visited Nov. 29, 2014).

291. *See Risks to consumers posed by virtual currencies*, CFPB (Aug. 2014), http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf.

292. *Id.*

has also begun accepting complaints about virtual currency products and services, including wallets and exchanges.[293]

Most Recently, the CFPB has proposed a rule to expand consumer protections to digital wallets, potentially including digital wallets for virtual currencies.[294]

d) State Regulation of Bitcoin: New York and California

On July 17th, 2014, New York became the first state to attempt to regulate Bitcoin by introducing a proposed licensing regime to operate in the state.[295] The New York State Department of Financial Services ("NYDFS") issued proposed rules to create requirements on exchanges and companies that secure, store, or maintain custody or control of virtual currency for customers.[296] Benjamin M. Lawsky, former Superintendent of Financial Services, characterized the "BitLicense" regulatory framework requirements as a "common sense rules of the road" to further consumer protection, ensure anti-money laundering compliance, and address the unique cyber security concerns of virtual currency.[297] The regulations do not apply to virtual currency miners, software developers, or merchants and consumers who utilize virtual currency solely for the purchase or sale of goods or services, or firms chartered under the New York Banking Law to conduct exchanges with the approval of the NYDFS.[298]

The regulations were published in the New York State Register's July 23, 2014 edition to begin a forty-five-day public comment period.[299]

---

293. *See Submit a complaint*, CFPB, http://www.consumerfinance.gov/complaint/#money-transfer (last visited Nov. 29, 2014).

294. *See* Proposed Rule, Docket No. CFPB- 2014-0031 32–34 (Nov. 10, 2014), *available at* http://files.consumerfinance.gov/f/201411_cfpb_regulations_prepai-nprm.pdf.

295. *NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms*, N.Y. STATE DEP'T OF FIN. SERVS. NEWS ROOM (July 17, 2014), http://www.dfs.ny.gov/about/press2014/pr1407171.html.

296. *Id.*

297. *Id.*; Former Superintendent Lawsky has specifically mentioned preventing another Mt. Gox. *See* Paul Vigna & Michael J. Casey, *BitBeat: Lawsky Outlines Changes to BitLicense*, WALL ST. J. (Oct. 14, 2014), http://blogs.wsj.com/moneybeat/2014/10/14/bitbeat-lawsky-outlines-changes-to-bitlicense/.

298. *Superintendent Lawsky Remarks on Revised Bitlicense Framework for Virtual Currency Regulation and Trends in Payments Technology*, N.Y. STATE DEP'T OF FIN. SERVS. NEWS ROOM (Dec. 18, 2014), http://www.dfs.ny.gov/about/speeches_testimony/sp1412181.htm.

299. *See NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms*, *supra* note 295.

Perhaps in a nod to the digital nature of Bitcoin, the NYDFS also published the regulations on Reddit and Twitter.[300] Although the rules would only apply to firms doing business in the Empire State, Gil Luria, an analyst with Wedbush Securities, noted that as the state has the largest concentration of financial firms, its regulatory and enforcement framework might serve as a model for other states, or even for the SEC or Federal Reserve.[301]

Key requirements for firms to obtain a BitLicense include: capital holding requirements with a bond or trust account in US dollars, providing receipts on transactions, establishing a complaint policy, providing consumer disclosures on the risks inherent to virtual currency compared to fiat currency,[302] compiling information on transactions for anti-money laundering compliance (essentially deanonymizing the parties involved), reporting fraud or suspicious activities, maintaining cyber security programs, designating a Chief Information Security Officer and Compliance Officer, being subject to NYDFS examinations, submitting quarterly financial statements, and establishing business continuity and disaster recovery plans, with notification to NYDFS during an emergency.[303]

On December 18, 2014, Lawsky outlined revisions to the BitLicense in light of the over 3,700 public comments submitted to the original proposal.[304] In response to complaints that the cost of compliance would discourage startups and small businesses, the regulations will include a two-year transitional BitLicense for companies unable to satisfy all the requirements of a full license.[305] Additionally, companies would no longer be required to obtain the addresses and transaction data for all parties to a transaction.[306] Instead, companies would only need to obtain this type of information on their own customers and account holders.[307]

---

300. *Id.*

301. Cyrus Farivar, *New York state proposes sweeping Bitcoin regulations—and they're strict*, ARS TECHNICA (July 17, 2014), http://arstechnica.com/tech-policy/2014/07/new-york-state-proposes-sweeping-bitcoin-regulations-and-theyre-strict/.

302. *Fiat Currency Definition*, *supra* note 44.

303. *NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms*, *supra* note 295.

304. *Superintendent Lawsky Remarks on Revised Bitlicense Framework for Virtual Currency Regulation and Trends in Payments Technology*, *supra* note 298.

305. *Id.*

306. *Id.*

307. *Id.*

Officials in California's Department of Business Oversight have also determined that a state law governing money transmitters may also apply to digital currencies, such as Bitcoin.[308] Spokesman Tom Dresslar indicated the requirements to obtain a California license would focus primarily on consumer protection.[309] Potential requirements include demonstrating sufficient capital to operate, having a qualified management team subject to criminal background checks, and being bonded at levels consistent with size.[310] Applicants would also have to maintain reserves equal to the amount of their outstanding money transmissions.[311] Notably, these regulations will come on the heels of a recently enacted California statute repealing a state law prohibiting the issuance of anything other than U.S. dollars in the state.[312] This statute grants Bitcoin the status of "lawful money" under state law along with rewards programs and coupons.[313]

C. BITCOIN-RELATED LITIGATION IN THE UNITED STATES

As federal and state agencies continue to tackle the regulation of Bitcoin, courts have been forced to define Bitcoin in the course of recent litigation. Below are four key cases shaping the government's stance on Bitcoins.[314]

What characterizes these cases is that judges have taken a functional view of Bitcoin and defined it on a case-by-case basis as necessary to hold defendants culpable. In the four cases below, all of the judges defined Bitcoin as money so as to subject it to the Securities Act, and state and federal money laundering statutes.

308. Michael B. Marois & Carter Dougherty, *California Says State Law Grants Right to Oversee Bitcoin*, BLOOMBERG.COM (Dec. 4, 2014), http://www.bloomberg.com/news/2014-12-04/california-says-state-law-grants-right-to-oversee-bitcoin.html.

309. *Id.*

310. *Id.*

311. *Id.*

312. CA A.B. 129 (2014) (repealing Section 107 of the Corporations Code).

313. Pete Rizzo, *California to Debate Bitcoin Regulation at December Meeting*, COINDESK (Dec. 5, 2014), http://www.coindesk.com/california-debate-bitcoin-regulation-december-meeting/.

314. Tanaya Macheel, *4 Court Cases Helping Shape the US Stance on Bitcoin*, COINDESK (Sept. 28, 2014), http://www.coindesk.com/4-court-cases-helping-determine-us-stance-bitcoin/.

1. *SEC v. Shavers*

Defendant Trendon T. Shavers founded and operated Bitcoin Savings and Trust ("BTCST"), which was subsequently declared a Ponzi scheme used to defraud investors by Magistrate Judge Amos Mazzant of the Eastern District of Texas.[315] Judge Mazzant found that Shavers used new Bitcoins received from BTCST investors to make payments on outstanding BTCST investments, while diverting investor Bitcoins for his personal use.[316] Judge Mazzant held that the investments sold by Shavers met the definition of investment contract and were thus securities, giving the court jurisdiction over the case through the Securities Act.[317]

In an earlier memorandum to establish the court's subject matter jurisdiction, Judge Mazzant declared Bitcoins to be a form of currency.[318] The Securities Act defines a "security" as "any . . . investment contract."[319] An investment contract is defined as "any contract, transaction, or scheme involving (1) an investment of money, (2) in a common enterprise, (3) with the expectation that profits will be derived from the efforts of the promoter or a third party."[320] Thus, the threshold question for the court was whether the Bitcoins invested into Shaver's Ponzi scheme qualified as an investment of money. Judge Mazzant reasoned that because Bitcoins can be used to purchase goods or services, pay for individual living expenses, and be exchanged for fiat currencies, Bitcoins constituted an investment of money.[321]

2. *United States v. Faiella*

In the Southern District of New York, Judge Jed Rakoff ruled in August 2014 that Bitcoins are money and were thus subject to FinCEN's regulations.[322] Defendants Robert Faiella and Charlie Shrem were accused of operating an unlicensed money transmitting business and conspiring to commit money laundering in connection with Silk Road.[323] The defendants moved to dismiss the indictment by arguing that Bitcoins did

315. *See generally* Secs. & Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2014 WL 4652121 (E.D. Tex. Sept. 18, 2014).
316. *Id.* at *8.
317. *Id.*
318. Secs. & Exch. Comm'n v. Shavers, 2013 WL 4028182 at *2 (E.D. Tex. Aug. 6, 2013).
319. *Id.*
320. *Id.*
321. *Id.*
322. United States v. Faiella, 39 F. Supp. 3d 544, 545–47 (S.D.N.Y. 2014).
323. *Id.* at 545.

not qualify as "money" under racketeering laws, and that operating a Bitcoin exchange does not constitute "transmitting money" and that the defendants were therefore not "money transmitters" under 18 U.S.C. § 1960.[324]

Judge Rakoff rejected the defendants' arguments, reasoning that Bitcoin clearly qualifies as "money" or "funds" using plain meaning definitions found in the dictionary as it "can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions."[325] The court found this definition consistent with the legislative history of § 1960, which was passed to prevent money laundering in connection with drug dealing.[326] The court also found that Congress chose to use the term "funds" to keep up with the evolving methods of money launderers.[327] Judge Rakoff went to further define the defendant's activities as "transmitting money" and thus qualifying them as "money transmitters" and subject to FinCEN's virtual currency guidance.[328]

3. *United States v. Ulbricht*

The Dread Pirate Roberts, a.k.a. Ross Ulbricht[329] also challenged the applicability of money laundering laws to virtual currency.[330] Judge Katherine Forrest ruled that as an initial matter the use of Bitcoins for payment is insufficient in and of itself to state a claim for money laundering, and that anonymous transactions are not crimes.[331] Instead, the basis of the charge was the use of Bitcoin to shield unlawful activities such as narcotics trafficking and, in Ulbricht's case, computer hacking from third party discovery.[332]

Ulbricht also brought a similar argument as the defendants in *Faiella*, arguing that Bitcoins did not qualify as "funds" for the purposes of money laundering statutes.[333] Judge Forrest found Ulbricht's argument unavailing, and by using similar reasoning to Judge Rakoff, she held that "money" and "funds" were simply methods to pay for things and thus the terms covered

324. *Id.*
325. *Id.*
326. *Id.* at 545–46.
327. *Id.* at 546.
328. *Id.* at 546–47..
329. *See supra* Section IV.B.1.b).
330. United States v. Ulbricht, 31 F. Supp. 3d 540, 548 (S.D.N.Y. 2014).
331. *Id.* at 568–70..
332. *Id.*
333. *Id.*

Bitcoins.[334] Judge Forrest noted that Bitcoins' "sole raison d'etre" was to pay for things, and any other reading would be "nonsensical."[335]

4. Florida v. Espinoza

Undercover agents arrested Pascal Reid and Michell Abner Espinoza in sting operations for converting $30,000 of cash in to Bitcoin through the online marketplace LocalBitcoins.com.[336] These charges represent the first-ever state prosecution of money laundering with virtual currency.[337] The defendants were charged under Florida's anti-money laundering law, which prohibits exchanges and business transactions of over $10,000 and the state's unlicensed money transmission law which sets a yearly cap of $20,000 on payment and currency instruments.[338]

The Bitcoin Foundation has filed an amicus brief arguing that the money transmission law applies to corporations and entities qualified to do business in the state and that the Florida statute is too ambiguous on virtual currency to be enforced.[339] The defendants have also moved for dismissal invoking the IRS's guidance that Bitcoin is property, not currency.[340]

V. SUGGESTIONS FOR THE FUTURE

Two things are necessary for the wider adoption of Bitcoin: it must become easier to use as a currency, and it has to shed its negative associations to gain the trust of average consumers. Bitcoin and the blockchain can change society in many ways, but the ideas proposed in Part II of this Note all depend on wider adoption. Bitcoins must be brought into the light and seen as a useful currency, and not simply the refuge of deep web denizens.

To promote these two goals, the regulators' tasks are twofold. First, regulators must seek to create a system where Bitcoins are treated solely as a currency, allowing consumers and merchants to feel more comfortable

---

334. *Id.* at 570.

335. *Id.*

336. Macheel, *supra* note 314.

337. Susannah Nesmith, *Miami Bitcoin Arrests May Be First State Prosecution*, BLOOMBERG.COM (Feb. 10, 2014), http://www.bloomberg.com/news/2014-02-09/miami-bitcoin-arrests-may-be-first-state-prosecution.html.

338. Macheel, *supra* note 314.

339. Pete Rizzo, *Bitcoin Foundation Urges Court to Dismiss Charge in Florida LocalBitcoins Case*, COINDESK (Aug. 1, 2014), http://www.coindesk.com/bitcoin-foundation-urges-court-dismiss-charge-florida-localbitcoins-case/.

340. Macheel, *supra* note 314.

relying on Bitcoin as a medium of exchange. Second, regulators must de-anonymize Bitcoin to rid the currency of its (perhaps rightfully earned) negative connotations.

To accomplish the first goal, the IRS's current policy of treating Bitcoin as property must change.[341] Requiring Bitcoin users to declare capital gains taxes on all their transactions is too cumbersome. The IRS's classification is not wholly irrational given Bitcoins' current popularity as an investment device, rather than a currency. Yet subjecting Bitcoins to a capital gains tax hampers the use of Bitcoins as a means of exchange. Therefore the IRS should either set a sunset date to their current classification or some objective criteria of price stability that would reflect a change in usage of Bitcoin from an investment tool to a currency.

To accomplish the second goal, Bitcoin users should register their public key addresses to their real identities. While some of the benefits of anonymity will be lost, it is a worthwhile tradeoff to both make illicit use of Bitcoin more difficult, and to build public confidence and acceptance. This is already happening to some extent with Bank Secrecy Act registration of Bitcoin exchanges with FinCEN. While such a change may drive away some of Bitcoins' initial users in the libertarian scene, the potential of Bitcoin and the blockchain are too great to be lost in an attempt to accommodate such idiosyncratic beliefs.[342] The benefits of expanding markets and lowering transaction costs cannot be subordinated to some people's desires to maintain anonymity in transactions. For consumers who really value such anonymity, they may, as they can today, use cash. There may be no way for the government to force compliance at the individual level as users can have multiple Bitcoin wallets, and thus multiple public key addresses. But through a mix of incentives and disincentives, many users might be convinced to comply. For example, the government could create tax incentives for people to register their public key addresses with the IRS. The government could also increase punishments against defendants who used Bitcoins to facilitate the commission of a crime. There is likely no way to fully deanonymize users of the blockchain, but to the extent that it is possible, it might increase consumer confidence, and thus adoption, of Bitcoin. This would also

341. *See supra* Section IV.B.2.a).

342. Some observers already believe the libertarian community will turn away from Bitcoin as members of the community begin to understand that the blockchain is public. *See* Kim-Mai Cutler, *Marc Andreessen: "My Prediction Is That The Libertarians Will Turn on Bitcoin,"* TECHCRUNCH (Mar. 25, 2014), http://techcrunch.com/2014/03/25/marc-andreessen-my-prediction-is-that-the-libertarians-will-turn-on-bitcoin/.

allow for other benefits, such as facilitating the passing down of Bitcoins in situations of intestacy, or escheating to the state when there is no next of kin.

VI. CONCLUSION

Trust is vital to the adoption of a payment service. As Supriya Singh observes: "there is nothing inherent in a piece of paper, a plastic card or electronic information that converts it into money."[343] Ultimately Bitcoin's wider adoption, and its attendant benefits, will come down to how much consumers trust it as a stable medium of exchange and token of value.

Bitcoin's bad actors, hackers, and black markets damage this trust. Smart regulation must protect us as, and sometimes from, Bitcoin users. Unmasking actors on the blockchain will help Bitcoin shed its infamous reputation and potentially revolutionize the way we conduct business, the size of the global market, and perhaps even our conception of what ownership means.

343. Singh, *supra* note 27 at 3.4.

1. Introduction

Virtual currency schemes have proliferated in recent years and have become a focal point of media and regulators. Virtual currencies are defined by the European Banking Authority as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to fiat currencies, but is used as a means of exchange and can be transferred, stored or traded electronically. [1]

This paper focuses on Bitcoin, the first decentralized variation of virtual currency. In 2008 the Bitcoin white paper was published online by Satoshi Nakamoto, a pseudonymous person or likely a group people. The paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" proposes a "purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution [..] a system for electronic transactions without relying on trust.[2] The open source Bitcoin software was released in January 2009, with an establishment of an exchange rate only on October 5, 2009 where 1 USD = 1,309 BTC. This initial value was calculated as the electricity exerted per bitcoin generated.[3] Since then, the system has grown to into a currency that is used for 60 – 80 thousand transactions per day, has a market capitalization of 5 billion USD, and trades 1 BTC = 380 USD.[4] Regardless of the extreme volatility in the exchange rate, an increasing number of suppliers are now accepting Bitcoin as a means of payment for a myriad of goods and services. Adopters include large multinationals companies such as eBay Inc's PayPal service, Dell Inc. (multinational technology corporation), DISH Network (pay-TV provider), CheapAir (airline) and Expedia Inc. (online travel agency, hotel bookings).[5]

The objective of this paper is to provide a description of the technical nature of Bitcoin and the reason for its existence. With an understanding of the basic workings of this new payment

---

[1] European Central Bank, 'EBA Opinion on 'virtual currencies', *EBA/Op/2014/08*. 2014.

[2] Nakamoto, S. 'Bitcoin: A Peer-to-Peer Electronic Cash system.', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

[3] 'New Liberty Standard', (accessed 10 October 2014), http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate

[4] It must be noted that 1 BTC is arbitrarily divisible by up to 10^8. Thus, every bitcoin represents 100 million "satoshis"

[5] Morphy, E. 'Bitcoin? Yawn. CheapAir Is Now Taking Litecoin and Dogecoin.', *Forbes*, 2014, (accessed 30 September 2014), http://www.forbes.com/sites/erikamorphy/2014/09/03/bitcoin-yawn-cheapair-is-now-taking-litecoin-and-dogecoin/

'What can you buy with Bitcoins?', *Coindesk*, 2014, (accessed 29 September 2014), http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/

system, we can draw comparisons to fiat currency, analyze the associated risks and benefits, and effectively discusses the current regulatory framework.

The second chapter introduces money theory. To understand Bitcoin, we require a basic understanding of the origin of money and role states and financial institutions play in the acceptance of money. It is accepted that the core objective of central banks is securing the stability of the national economy (price stability), and thus the stable value of a currency through maintaining public trust in the currency.[6] The bitcoin protocol autonomously determines how new bitcoins are created and the total possible number of bitcoins is fixed. This precludes the possibility of state intervention its supply and thus, questions the role of the state.

The third chapter describes and technical and economic nature of Bitcoin, drawing a comparison between its key properties to fiat currency systems. This chapter will provide a translation of the technical aspects of Bitcoin system which must be understood before its regulation can discussed.

The fourth chapter describes the potential economic and conceptual benefits of decentralized virtual currencies, followed by chapter five which will identify risks arising from the use of virtual currencies. Risks will be categorized according to the bearer of the risk (users, non-user market participants, financial integrity, etc.).[7]

Chapter six will discuss the regulation of virtual currencies. The regulatory vacuum Bitcoin once existed in is swiftly getting filled with varying sentiment, while most countries adopt a *permissive* stance, others outright ban it. Regulation is required to safeguard parties within the virtual currency ecosystem from various risks that accompanies its use. Decentralized virtual currencies face particularly challenging law enforcement predicaments because of their ability to disregard national borders while having no "owner" that controls the system, thus systems like Bitcoin, cannot be tied to any single jurisdiction.

Chapter seven concludes by mentioning noteworthy future applications of distributed ledger technology, and argues that the inventions underlying Bitcoin may change the world for the better.

[6] Committee on Payment and Settlement Systems, 'The role of central bank money in payment systems', *Bank for International Settlements*, 2003.

[7] European Central Bank, 'EBA Opinion on 'virtual currencies', *EBA/Op/2014/08*, 2014.

2. The evolution of money

2.1 Defining money

Money is a surprisingly elusive concept. Bamford(2011) stated that as with most attempts to define intellectual constructs, definitions of money describe what it does and some characteristics it has, instead of aiming to describe the thing itself.[8] In human societies throughout history, money has served as commodities or tokens that have value and is used as a medium of exchange.[9] Money's source of value stems from society's general agreement of what is seen acceptable tender in making payments and settling debt, rather than physical characteristics of the chosen media used.[10]

Classical economists agree that money mainly serves three functions within an economy. Firstly as a 'medium of exchange': An item that facilitates the exchange, something buyers give to sellers as payment for goods or services. Secondly as a 'unit of account': a benchmark used by people to measure and record economic numerically. Thirdly as a 'store of value': an item used to transfer purchasing power from the present into the future.[11]

Money that performs the abovementioned functions effectively usually has fairly uniform qualities. Jevons(1875) identifies properties such as: portability, must be convenient to store and transport; indestructability, must not deteriorate over time; homogeneity, units must be fungible; divisibility; and cognoscibility, units must be easily recognizable and secured from any counterfeiting.[12]

2.2 The Origin of Money

Money, as social institution, is used in almost every human society to facilitate trade. Trading allows standards of living that would not be possible if individuals were expected to independently produce every single commodity that they require. Before the existence of money, all exchanges had to take place through barter. Barter trade is typically a bilateral

---

[8] Bamford, C, *Principles of International Financial Law*, Oxford: Oxford University Press, 2011, pp. 10.

[9] Eatwell, J., Milgate, M., & Newman, P. (1994). *The new Palgrave dictionary of economics*, London:Macmillan, 2008, pp. 725.

[10] *Ibid.*

[11] Mankiw, N. G. & Taylor, P.M., *Economics. 2nd ed*. Andover : South-Western Cengage Learning, 2011, pp. 618.

[12] Jevons, W. S. 'Money and the Mechanism of Exchange'. *Library of Economics and Liberty.* 1876. (accessed 28 October 2014). http://www.econlib.org/library/YPDBooks/Jevons/jvnMME5.html

exercise, requiring that parties to the trade have a *double coincidence of wants*.[13] This means the chicken farmer can *only* acquire milk, if the cattle farmer wants eggs. This problem is theoretically solvable through multilateral barter (A supplies B, B supplies C and C supplies A), but as these trades could not practically all happen at a single point in time, this system would still require a central clearing house to keep track of balances of traders. In a multilateral barter system, traders would not be required to be balanced with every other trader, but due to the absence of money, each trader would have to be balanced in every commodity. Each trader would have to keep a portfolio of numerous goods which must not only be taken to each trading session, but must also be constantly synchronized by the clearing house.[14] This system would be clumsy, inefficient and extraordinarily complex.

Now we can consider how money acts as a lubrication to barter. By using money, traders are able to transfer purchasing power from one transaction to the next, overcoming the absence of *a double coincidence of wants* without a complex multilateral barter system. Traders have a reduced need for information and co-ordination and trades are subject to lower transaction costs. Buyers only need to know that sellers will accept money as payment. Money enables simpler pricing of goods, by allowing traders to assign a numerical value to each commodity in the common medium of exchange (as opposed to the value of each good being expressed in terms of a variety of other goods).[15]

Once in place, the benefits of a monetary trading system are apparent, but a paradox remains- the paradox of monetary trade. How do economies gravitate towards such a system? A system where a seller in a transaction gives up something desirable (goods or services) for something without immediate use (money), trusting the idea that a future sellers will do the same.[16] Starr(2003) summarizes the paradox:

> Inconvenience of barter is the reason why monetization of trade is efficient but it does not explain why monetary trade is a market equilibrium, the self-confirming behavior of rational self-interested economic buyers and sellers. No agent can choose individually to monetize; monetization is the common outcome of the equilibrium of the trading process. Monetary trade requires voluntary co-ordination among

[13] Jevons, W. S. 'Money and the Mechanism of Exchange'. *Library of Economics and Liberty.* 1876. (accessed 28 October 2014). http://www.econlib.org/library/YPDBooks/Jevons/jvnMME5.html

[14] Eatwell, J., Milgate, M., & Newman, P.,*The new Palgrave dictionary of economics*, London:Macmillan, 2008, pp. 725.

[15] *Ibid.*

[16] Starr, R. M, 'Why is there money? Endogenous derivation of "money" as the most liquid asset: A class of examples.', *Economic Theory*, *21(2/3)*, 2003, pp. 455-474.

> households and firms. All must undertake to trade in the common medium. But it is by no means obvious that households and firms will voluntarily choose to trade in the commonly accepted money. [..] How can this arrangement be voluntarily sustained? [17]

There are two broad explanations for this paradoxical equilibrium- the Metallist(M) theory and the Chartalists(C) theory. These two views on the origin of money have been greatly debated in academia, and referred to as "the two concepts of money".[18]

2.3 The Two Concepts of Money

First the *Metallist* view, where a monetary trading system is the natural equilibrium resulting from the actions of self-interested parties in a free market barter economy, an endogenous process driven by the private sector with the purpose of minimizing the transaction costs related to trade.[19] Metallists focus on the medium of exchange function of money.[20]

The second theory is the *Chartelist* view, which argues that the state implements a monetary system as a means to facilitating the fiscal basis of government, money.[21] Chartalists recognize the power of the state to mandate that certain payments be made to it combined with the ability to determine the medium in which these payments must be made. The C theory provides a non-market-based theory where the currency is valued (and thus used) according to its usefulness in settling liabilities towards the state. Chartalists focus on the unit of account function of money. The state is the central force in the development of a monetary system, and the actual properties determining efficiency as a medium of exchange is irrelevant.[22]

M theory advocates most often quote the work of 19th century Austrian economist Carl Menger, which Starr(2001) refers to as a theory of market liquidity that forms the basis of

[17] Starr, R. M., 'Money: in transactions and finance'. *Dept. of Economics, University of California, San Diego*, pp. 13-15.

[18] Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas.' *European journal of political economy, 14*(3). 1998., pp. 407-432.

[19] *Ibid.*

[20] Bell, S., 'The Hierarchy of Money'.*TheJerome Levy Economics Institute. Working paper No. 231.* 1998.

[21] Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas.' *European journal of political economy, 14*(3), 1998, pp. 407-432.

[22] Bell, S. 'The Hierarchy of Money', *The Jerome Levy Economics Institute. Working paper No. 231*, 1998.

monetary theory. [23] Menger's theory stems from the concept that commodities in a barter economy have varying degrees of *saleableness* (meaning marketability or liquidity): "A commodity is more or less saleable according as we are able, with more or less prospect of success, to dispose of it at prices corresponding to the general economic situation, at economic prices."[24] Menger argues that since individuals within a barter economy recognize that certain commodities are relatively easier to trade compared to others, traders would acquire quantities of these commodities exceeding personal demand in order to better their chances of finding a suitable trading partner. These individuals' actions would have a network effect (increasing demand for the good results in further increasing demand) and further increase the *saleableness* of these commodities, further lowering the associated transaction costs. This process results in the most *saleable* commodity becoming accepted as a universal medium of exchange- the commodity with certain favorable characteristics, evolving into money.[25] Surda(2014) states:

> The core prerequisite for the classification as a medium of exchange is, for a casual observer maybe somewhat paradoxically, not the double coincidence of wants between the buyer and the seller with respect to the medium of exchange. Rather, it is the willingness of the buyer to hold it prior to the act of trading as a part of his liquidity portfolio.

The M perspective of the origin of money provides an explanation the process of how new commodities become a viable alternative medium of exchange. In a competitive environment that constantly strives towards lowering transaction costs, traders would naturally prefer a means of exchange which performs the functions of money more efficiently.[26]

While Menger attributes the origin of money to market forces, Menger recognizes the importance of the state in the historical development of money.[27] In Menger's monetary theory, state institutions aid the market with informational difficulties associated of using precious metals as money. Using precious metals in a raw form is inefficient as individuals are required to determine the true value of each unit they encounter. Through minting the raw

---

[23] Starr, R. M., 'Why Is There Money? Endogenous Derivation of "money" As the Most Liquid Asset: A Class of Examples.' *Economic Theory* 21.2/3. 2003, pp. 455-474.

[24] Menger, C., 'On the Origins of Money'. *Economic Journal, Vol 2*, 1892, pp. 239-255.

[25] *Ibid.*

[26] Olafsonn, I. A., 'Is Bitcoin Money?: An analysis from the Austrian school of economic thought'. *Haskoli Islands University*, 2014. pp 30.

[27] Ikeda, Y., 'Carl Menger's Monetary Theory: A Revisionist View'. *Keio University, Department of Economics*, 2008. pp 5.

materials into coins, traders are able to use trust the quality guarantee stamp of the mint, overcoming this informational difficulty.[28] Once the technology is available, the private sector is technically capable of minting yet the task is mostly a state-run operation.[29] The state plays this role for two reasons. Firstly, as public protector of law and order by means of force, the state is able to ensure the protection of the mint's inventory from theft. Secondly, in order to maintain trust in the quality of coins, the state ensures the value over time. A private mint operator "is bound to claim that the quality will be maintained forever, but in practice will always be tempted to debase the currency in pursuit of a quick and immediately larger return."[30] The state guaranteed the physical integrity of coins, solving the informational difficulties (lowering transaction costs) faced by individuals to trusting their real value.

Modern states guarantee the value of their own paper fiat money by declaring it as *legal tender* of the geographical area. Users are able to trust the government will accept fiat money as the only legal means of discharging financial obligations towards the state such as taxes or penalties. As long as tax obligations persist, the private sector will necessarily prefer fiat currency as payment in transactions.[31] Under the M approach, this property is seen an element to be considered by individuals choosing a preferred means of exchange. However, the combination of the state's ability to control the supply of fiat currency, and the power to impose taxes payable that fiat currency changes the role of the state in the equilibrium.

Here lies the core difference of the C perspective. The C theory views money as a *creature of the state* and views the state as the source of fiat money having value (rather than a contribution to its value), its value being primarily determined by its usefulness in extinguishing tax and other liabilities to the state.[32] Goodhart (1998) states:

> "[the] issue between the M and C theorists is how much of the subsequent acceptance of fiat money is due to the power of government, e.g., to impose taxes (C theory)., or to network factors and inertia encouraging people, without prompting from government, to stay with the existing currency (M theory) [..] Quite a number of economists combine the belief that M-form cost-minimization search theory

---

[28] Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas', *European journal of political economy, 14*(3), 1998, pp. 417-420.

[29] *Ibid:* In those cases where the mint has been run by the private sector, the government has in most cases both set the standards of fineness and extracted a rent, or seigniorage tax, that collected most of the available profits.

[30] Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas', *European journal of political economy, 14*(3), 1998, pp. 417-420.

[31] Bell, S. 'The Hierarchy of Money'.*TheJerome Levy Economics Institute. Working paper No. 231.* 1998.

[32] *Ibid.*

explained the initial development of money, but that more recently, the State has clearly taken over the provision of fiat currency. So, whether, or not, they like the result, they accept that the C-form theory is at present, more realistic.[33]

Money is no longer something that exists independent of the state; it is now a pillar of the sovereign.[34] Modern C theorist Minksy (1986) views money as a ledger or two-sided balance sheet, where the creation of money is contingent to the acceptance of another's debt.[35] Bell states that only the C theory views the "creation of money as a two-sided balance sheet operation where the acceptance of another's debt is possible.[36] When a state declares that all payments to it must be made in a certain means of payment, it creates a potential debtor. The debtors demand for this specific money implies the creation of money and gives rise to a creditor.[37] The initial way to inject its fiat currency is through government spending. Therefore the C approach argues that the functions of money as a means of payment and media of exchange are a derived from the principle function as a unit of account in which state obligations must be paid.[38]

Both theories recognize the possibility of several types of money co-existing in a market. Under the M theory commodities are *all* seen as potential forms of money, each with varying degrees of liquidity. C theorists have noted the existence of a 'hierarchy of money' or a 'debt pyramid', where state issued currency ranks highest since as their imposed "liabilities reign supreme as the only promises in the hierarchy which cannot be refused."[39] As a technological innovation allows the introduction of virtual currency schemes, a new stateless variation of potential money enters the market, bringing new benefits and risks to the table.

2.4 What are Virtual currencies?

Virtual currency schemes have proliferated in recent years and have become a focal point of media and regulators. Virtual currencies are defined by as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to fiat currencies, but is used as a means of exchange and can be transferred, stored or traded

[33] Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas', *European journal of political economy, 14*(3), 1998, pp. 417.

[34] *Ibid.*

[35] Bell, S. 'The Hierarchy of Money'.*TheJerome Levy Economics Institute. Working paper No. 231*. 1998.

[36] *Ibid.*

[37] *Ibid.*

[38] Semenova, A. 'The Origin of Money: Enhancing the Chartalist Perspective'. *CFEPS*. 2007.

[39] Bell (1998) summarizes the views of (Minsky, 1986; Foley, 1987; Wray, 1990)

electronically. In contrast to fiat currencies, virtual currencies are not legal tender but are nevertheless accepted by members within a virtual community as a medium of exchange and as a unit of account. Virtual currencies must also be distinguished from electronic money such as PayPal or Ven. In electronic money schemes the link between the electronic money and fiat currency is guaranteed through some legal foundation and funds are shown in the same unit of account (U.S. dollar, Euro, etc.).[40] Virtual currency schemes create an independent unit of account, which only exists in a digital form (Bitcoin, Litecoin, Ripple, etc.), which can be used as an alternative to fiat currency, or may be converted to fiat currency.[41]

In a broad sense there are two types of virtual currency schemes- centralized and decentralized. Centralized virtual currencies predate decentralized variations. Centralized virtual currencies have a centralized repository and is typically issued and controlled by a single organization. Decentralized virtual currencies have no central repository and are issued and operated in a decentralized manner. [42]

Centralized virtual currencies can be divided into three categories. Firstly, closed virtual currency schemes that are not convertible to fiat currencies (Frequent flyer miles, loyalty points and currencies typically used in online games such as World of Warcraft) and cannot be used for purchases outside the virtual community within which it exists. Secondly, unidirectional convertible virtual currencies (Linden Dollars or the Facebook credits) that are purchased at a fixed exchange rate (but cannot be converted back into fiat currency) and is typically used for the purchase of virtual goods or services. Thirdly, bidirectional convertible virtual currencies (Liberty Dollar, WebMoney, etc.) that allow buying and selling virtual currency according to the exchange rates with fiat currency. Bidirectional virtual currencies act similar to any other convertible currency and allows for the purchase of both virtual and real goods and services.[43]

The focus of this paper is on the decentralized variation of virtual currencies, the first variation of which emerged in 2009: Bitcoin. Through the innovative use of various

---

[40] European Central Bank,.'Virtual Currency Schemes', 2012, pp 11-14. (accessed 10 Ocotber 2014), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[41] European Central Bank,.'Virtual Currency Schemes', 2012, pp 11-14. (accessed 10 Ocotber 2014), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[42] FinCEN, 'Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury', *United States Financial Crimes Enforcement Network*, 2013.

[43] European Central Bank. 2014. "EBA Opinion on 'virtual currencies'.

technologies, decentralized virtual currencies allow online payments to be sent directly from one party to another, using a system based on cryptographic proof instead of trust.[44]

3. Decentralized Cryptographic Virtual Currency: Bitcoin

3.1 What is Bitcoin?

Bitcoin is an invention of a computer programmer using the pseudonym Satoshi Nakamoto.[45] This invention is open source, meaning its underlying computer code is free and open to public viewing. Bitcoin is a peer-to-peer network that uses cryptography to allow the secure transfer of unique digital assets (bitcoin) between any two parties in a decentralized manner (independent of a trusted third party).[46] Within this system, each transfer of bitcoin is visible to the entire network and is the legitimacy of each transfer is unchallengeable.[47]

Centralized virtual currencies require trust on a third party to regulate the creation of new units, to verify transactions, and update the ledger of account balances. Bitcoin precludes the need to trust a third party, by providing a solution to two long-standing problems in computer science which have plagued past forms of electronic value transfer: the double-spending problem and the Byzantine Generals Problem.[48] The innovative solution that allow Bitcoin to function as a peer-to-peer payment system, is the use of a global public ledger (the block chain), which is maintained and secured by the collective processing power of individuals in network.

The basic functioning of the Bitcoin network will be described in section 2.2, followed by an analysis of bitcoin units and bitcoin transactions in section 2.3. With this basic understanding

---

[44] Nakamoto, S., 'Bitcoin: A Peer-to-Peer Electronic Cash system', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

Cryptography is a branch of mathematics based on the transformation of data, which provide high levels of security.

[45] This paper distinguishes between *Bitcoin* (with an uppercase 'B') which refers to the protocol, network, or the system as a whole, and *bitcoin* (with a lowercase 'b') for the currency units (abbreviated as BTC).

[46] 'Cryptography'. (accessed 5 October 2014), https://bitcoin.org/en/vocabulary

[47] Nakamoto, S. 'Bitcoin: A Peer-to-Peer Electronic Cash system.', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

[48] Dourado, E & Brito, J. 'Cryptocurrency, The New Palgrave Dictionary of Economics'. Eds. Steven N. Durlauf and Lawrence E. Blume, Palgrave Macmillan, 2014, *The New Palgrave Dictionary of Economics Online*, Palgrave Macmillan. 20 October 2014. (accessed 20 October 2014). http://www.dictionaryofeconomics.com/article?id=pde2014_C000625

of how the Bitcoin system functions, section 2.4 will address questions such as why people use this system as a means of exchange, while providing an outline of the associated risks and benefits.

3.2 The Bitcoin System: How is a Global Public Ledger Maintained through Distributed Consensus?

The double-spending problem exists in all payments apart from physical cash. Once physical cash changes hands between Alice and Bob, it is final and all parties are aware of whose money it is[49]. With any form of electronic value transfer (simply information) it is not as apparent: Alice could simply copy the information and use it as payment for several transactions, ensuring each recipient that they are the new rightful owner. Unless Bob can trust Alice's word that she has "deleted" the cash from her account, this system cannot function. Prior to Bitcoin, the double-spending problem was solved by entrusting a third party intermediary to maintain a ledger of all account balances and transactions. The trusted third party confirms identities and updates balances as Alice requested.

Bitcoin invented a way to transfer (not copy) digital assets through the innovative use of public-private key cryptography and a peer-to-peer networking system. Bitcoin provides a distributed ledger called the block chain, a public record of all Bitcoin transactions in chronological order. The block chain is not maintained by a central authority, but is instead maintained in an automated manner by using the network's combined computing power to verify balances and secure transactions.[50] Valid requested transactions form blocks which, once confirmed, are linearly added to the chain (every 10 minutes on average).[51] Transactions can only be requested by the party that holds the password (private key) associated with an account (public key).[52] After confirmation of every block, all nodes automatically update their version of the block chain.

But distributing the ledger between all nodes brings the second problem: The Byzantine Generals Problem. This problem is specifically about asynchronous communications:

[49] It is final in the sense that the only way to reverse the transaction would be that Bob give it back to the Alice.

[50] Anyone with internet access is able to download the open-source software and contribute processing power to the network.

[51] http://blockchain.info/blocks

[52] (accessed 5 October 2014), https://bitcoin.org/en/vocabulary

> The Byzantine Generals Problem is abstractly stated as: a set of generals must agree on a common battle plan using only messages to communicate; it is known that there may be traitors trying to sabotage the messages. The loyal generals must decide on the same plan of action. Moreover, the loyal generals should not be coerced into adopting a bad plan by the traitors. More concretely, a system must be reliable even with malfunctioning components.[53]

This problem applied to the Bitcoin network, raises the following questions. When nodes receive an updated version of the block chain, how can they be sure that it is not a falsified update? In other words, how can distributed parties who do not trust each other reach consensus on the current state of the block chain? [54] Bitcoin's solution is the process of "mining". Mining is a distributed consensus system that is used to confirm waiting transactions by including them in blocks added to the block chain.[55] This process of the network achieving consensus is called "mining" as it is also the source of newly minted coins, which serves as incentive to miners to dedicate resources to validate transactions and to secure the network.

Miners are defined as nodes in the network which provide processing power to collect valid transaction requests and assemble blocks that are added to the block chain. The miners function competitively, each receiving all transactions and independently attempting to assemble a valid block (1 miner succeeds approximately every 10 minutes).

The miner that "found" the valid block first, is rewarded for his processing power contribution. The incentive is two-fold: New coins that the Bitcoin protocol issues as a bounty, and transaction fees from all transactions included in the block.[56] The new coins rewarded by the protocol are the only way the coins in circulation increases. The total supply of bitoins is fixed at 21 million, and the coins enter circulation in a predetermined decreasing rate. The current reward is 25 BTC per block, and halves every 210,000 blocks (roughly every 4 years) until the reward equals 1 satoshi (the smallest possible part of a bitcoin, 0.00000001

---

[53] Lamport, L., Shostak, R and Pease, M., 'The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems', July 1982, pages 382-401, as summarized by Jacobson, E. (accessed 6 October 2014), http://pages.cs.wisc.edu/~swift/classes/cs739-sp11/blog/2011/02/the_byzantine_generals_problem.html

[54] Dourado, E & Brito, J. 'Cryptocurrency, The New Palgrave Dictionary of Economics'. Eds. Steven N. Durlauf and Lawrence E. Blume, Palgrave Macmillan, 2014, *The New Palgrave Dictionary of Economics Online*, Palgrave Macmillan, 2014, http://www.dictionaryofeconomics.com/article?id=pde2014_C000625

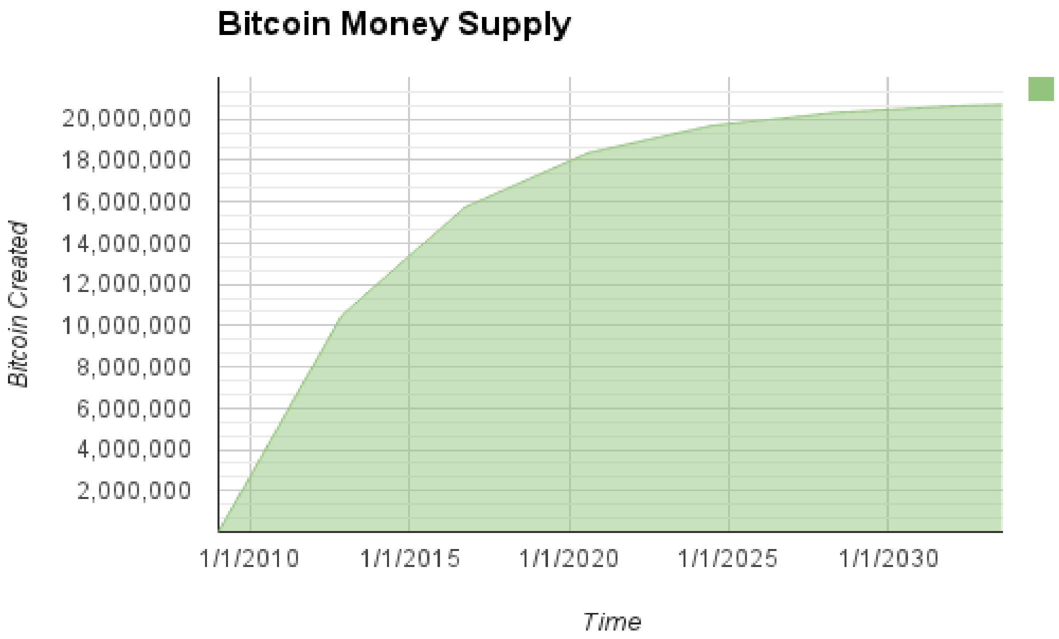
[55] 'How does Bitcoin work?' (accessed 10 October 2014). https://bitcoin.org/en/how-it-works

[56] (accessed 5 October 2014). https://en.bitcoin.it/wiki/How_bitcoin_works

BTC). After that block, roughly 2140, the reward will consist only of transaction fees. The supply of bitcoins is thus expanded at a decreasing rate, as shown in figure 1.

As the total supply and the rate at which the coins enter circulation are fixed, the system is protected from an oversupply of currency (hyperinflation). This has been referred to as digital scarcity.

Figure 1. Supply of bitcoins over time



The process of producing a valid block is intentionally difficult (time consuming), and is like a competition between miners to solve a complex mathematical puzzle (based on a cryptographic hash function). The solution to this puzzle, called “Proof-of-Work”, forms part of each block and functions as evidence that the miner expended significant computing effort to produce the block.[57] The network automatically adjusts the difficulty so to ensure than an average of 6 blocks are found per hour (The more miners attempting a solve it, the more difficult it becomes), resulting in the predetermined rate of the expansion of the monetary supply. Cryptographic hash function puzzle have special qualities and can be described by a useful analogy drawn by Antonopolous (2014):

> [M]ining is like a giant competitive game of sudoku that resets every time someone finds a solution and whose difficulty automatically adjusts so that it takes approximately 10 minutes to find a solution. Imagine a giant sudoku puzzle, several thousand rows and columns in size. If I show you a completed puzzle you can verify it

[57] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies.* O’Reily Media. 2014.

> quite quickly. However, if the puzzle has a few squares filled and the rest is empty, it takes a lot of work to solve! The difficulty of the sudoku can be adjusted by changing its size (more or fewer rows and columns), but it can still be verified quite easily even if it is very large. The "puzzle" used in bitcoin is based on a cryptographic hash and exhibits similar characteristics: it is asymmetrically hard to solve but easy to verify, and its difficulty can be adjusted.[58]

This analogy provides a useful glimpse into the intricacies of Bitcoin's innovative use of cryptographic hash functions and helps explain the role of miners. The first miner to produce a valid block broadcasts it to the rest of the network which easily recognizes that the broadcasted block is valid, updates their copies of the block chain by adding the new block, and immediately starts working on the next.[59] One ingredient used in producing each block, is the previous block's fingerprint, and thus each block confirms the integrity its predecessor-all the way back to the genesis block.[60] If any changes would be made to any blocks, all subsequent blocks would no longer make sense and would instantly be spotted by other nodes, and simply not be accepted. This is the source of the networks security, as any changes to previous blocks would require to redo the Proof-of-Work for all subsequent blocks, which becomes exponentially difficult for each block that is added. The network views only the longest chain of blocks as valid, as it is the chain supported by the majority of the network's processing power. After a few blocks have been added, users can trust that transactions have taken place irreversibly and no question of ownership remains.[61]

But how does this solve the Byzantines Generals Problem? Imagine two miners solve the puzzle at almost exactly the same and each node in the network must decide which for themselves which the chain is the correct one that should be further extended. Nakamoto(2009) frames the problem and explains Bitcoin's solution:

---

[58] Antonopoulos, A. M., *Mastering Bitcoin: Unlocking digital crypto-currencies,* O'Reily Media, 2014, (accessed 14 October 2014), http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#_public_key_cryptography_and_crypto_currency

[59] Pacia, C., 'Bitcoin Mining Explained Like You're Five: Part 1 – Incentives', 2014, (accessed 10 October 2014) http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-1-incentives/

[60] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies.* .O'Reily Media, 2014, (accessed 14 October 2014), http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#_public_key_cryptography_and_crypto_currency

[61] Nakamoto, S. 'Bitcoin: A Peer-to-Peer Electronic Cash system.', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

> The problem is that the network is not instantaneous, and if two generals announce different plans at close to the same time, some may hear one first and others hear the other first.
>
> They use a proof-of-work chain to solve the problem. Once each general receives whatever plan he hears first, he sets his computer to solve a difficult hash-based proof-of-work problem that includes the plan in its hash. The proof-of-work is difficult enough that with all of them working at once, it's expected to take 10 minutes before one of them finds a solution and broadcasts it to the network. Once received, everyone adjusts the hash in their proof-of-work computation to include the first solution, so that when they find the next proof-of-work, it chains after the first one. If anyone was working on a different plan, they switch to this one, because its proof-of-work chain is now longer.[62]

In the sense of the Byzantines Generals Problem, a loyal miner can be trust the longest chain as the true order of events, since at least 51 percent of the loyal miners have already agreed upon it.

Thus, mining is the system that confirms waiting transactions, maintains the state of the ledger, protects the neutrality of the network, and also distributes new bitcoins in predetermined manner. The system is designed to incentivize individuals, acting as rational self-interested parties, to contribute processing power towards the operation and security of the network. These individuals are not required to trust each other, and through mining they are able to reach consensus.

It must be noted that the system itself is not a currency, but rather that the system (i.e. the block chain and mining) forms the basis on which bitcoins can be used as currency. The next questions are: what is a bitcoin (the unit that is transferable using the network)? ; how are bitcoins stored?; and what is a bitcoin transaction?

3.3 Wallets, bitcoins and Transactions

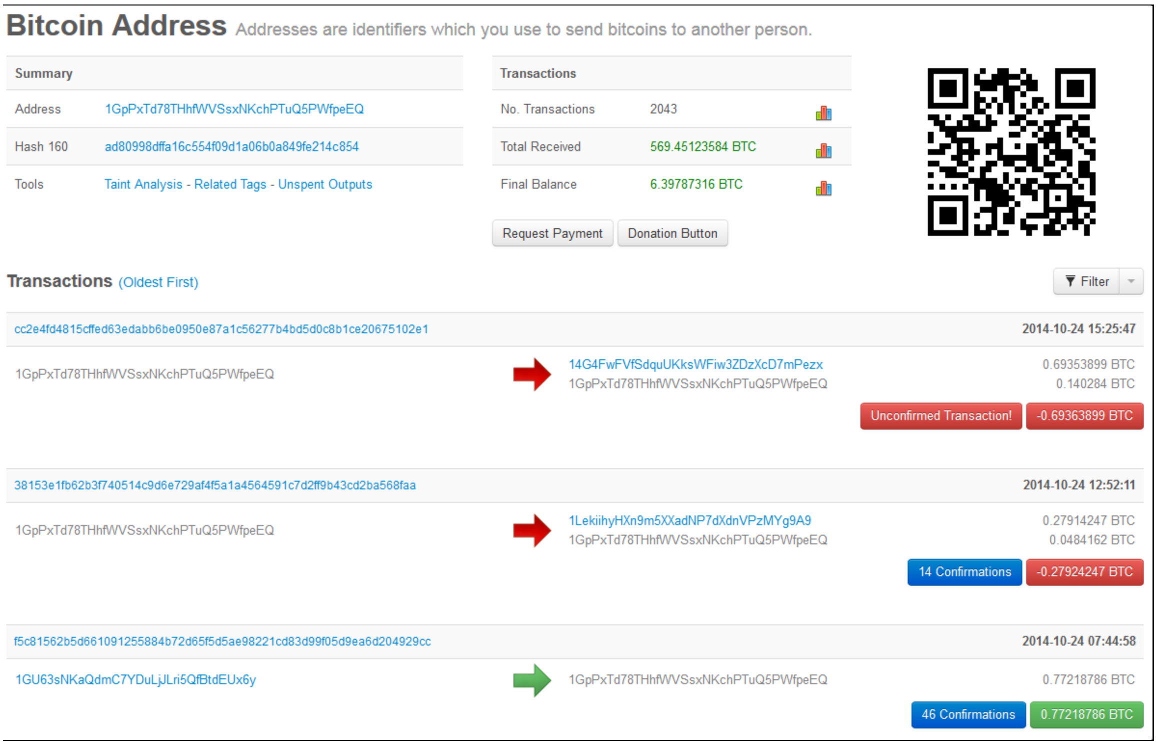
Nakamoto(2008) defines bitcoins as a chains of digital signatures.[63] Each owner transfers the bitcoin to the next, by digitally signing a hash of the previous transaction and the bitcoin address of the next owner and adding these to the end of the coin. The bitcoin address of the

[62] Bitcoin Forum Post by Satoshi Nakamoto, 2014, (accessed 15 October 2014), https://bitcointalk.org/index.php?topic=99631.0

[63] Nakamoto, S. 'Bitcoin: A Peer-to-Peer Electronic Cash system.', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

recipient is the only information the owner requires to initiate a transfer. Bitcoin addresses are public, anyone can see the entire transaction history and final balance on the block chain by using block chain explorer websites (figure 2). Bitcoin is said to be pseudonymous as Bitcoin addresses that are recorded in the block chain are not explicitly tied to anyone's identity. However, if a user makes a single transaction which links his/her identity to the address, it is easy to link the user's identity to all transactions associated with the address through the block chain.

Figure 2: Bitcoin address[64]



Source: https://blockchain.info/address/1GpPxTd78THhfWVSsxNKchPTuQ5PWfpeEQ

3.3.1 Digital keys, Addresses and Wallets

Addresses are derived from public keys, which are derived from private keys, and each derivation uses a one-way mathematical function. The public-private key pair is mathematically related in such a way that each private key has a unique public key. A private key is simply a randomly generated number, which is used to create digital signatures required to spend bitcoins.[65] Generating a unique private key is cost free, there are no limitations regarding to the amount of key pairs users can create, and does not even require an

---

[64] https://blockchain.info/address/1GpPxTd78THhfWVSsxNKchPTuQ5PWfpeEQ

[65] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies*, O'Reily Media, 2014, (accessed 14 October 2014). http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#_public_key_cryptography_and_crypto_currency

internet connection.[66] Private keys must be kept secret and stored safely since funds that are held in associated addresses, can only be spent with the private key. If the private key is lost, the bitcoins held in addresses associated with it are locked in the address forever. As mentioned, a private key can be generated offline. This means that users do not really create a private key, but simply *chooses* one from the existing pool at random. The number of possible private keys is so immense (2^{256}, which is a 1 with 77 zeros) that it is virtually impossible to randomly generate the same private key twice.

A bitcoin address usually represents the owner of a private/public key pair, but can also represent something else such as a payment script.[67] Currently, the most commonly implemented type of payment script address is multi-signature addresses. Multi-signature addresses require a certain number of the parties associated with the address to sign transactions in order to spend the funds. Antonopoulos(2014) gives two examples of how multi-signature addresses can be used:

> […] could use multi-signature address requiring 1-of-2 signatures from a key belonging to him and a key belonging to his spouse, ensuring either of them could sign to spend a transaction output locked to this address. This would be similar to a "joint account" as implemented in traditional banking where either spouse can spend with a single signature.
>
> [...] a 2-of-3 multi-signature address for his business that ensures that no funds can be spent unless at least two of the business partners sign a transaction.[68]

This is just one example of addresses that can be used as to create a form of corporate governance control that can protect funds against theft or loss.[69]

Bitcoin users store their key pairs in wallets. Wallets can be either be self-managed and stored on a mobile device, desktop computer, hardware wallets or even paper wallets; or can be in a

---

[67] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies.* .O'Reily Media, 2014. (accessed 14 October 2014). http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#_public_key_cryptography_and_crypto_currency

[68] *Ibid.*

[69] Antonopoulos, A. M., *Mastering Bitcoin: Unlocking digital crypto-currencies.* .O'Reily Media, 2014. (accessed 14 October 2014). http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#p2sh

on a third party's server and accessed online. When storing a wallet on your home computer or mobile phone it must be kept in mind that bitcoins are like real money, and that there is no central party to reimburse you in case of loss or theft. Users keeping their coins on their computer or mobile device thus require the technical knowledge to secure their devices. For the average computer user who assumes there is no malicious software on his computer (because Norton's Antivirus declared it so), these self-managed software wallets will not suffice. The more user-friendly option is to use web wallet services, where a third party is entrusted to keep users keys secure and users simply log into their website or mobile application to access their wallet and in some cases the storage services even insures against theft and loss.[70]

Since Bitcoin acts similar to cash it is advised to only keep day-to-day funds in an online wallet, and the rest in offline hardware or paper wallets (cold storage). As previously mentioned, private keys can be generated offline, and be stored in a hardware wallet (Trezor) or a paper wallet. This way, users are able to create private keys that have never been connected to the internet and are never stored on hardware that will be connected to the internet, making their bitcoins immune to cyber-attacks. Bitcoins stored in cold storage require *at least* physical access to the wallet in order to control the funds.

3.3.2 bitcoins

The next step is to investigate the tokens that are storable and transferrable on the Bitcoin system: bitcoins. Due to a fixed eventual money supply of 21 million, bitcoins are scarce by design. Bitcoins are also impossible to counterfeit. This is an attractive property cited by advocates when comparing Bitcoin to fiat currencies: For example in the 2013-2014 fiscal year almost $90 million counterfeit U.S. dollars were seized by the secret service, who made 3,617 counterfeiting arrests.[71] Bitcoins can be transferred online or offline (by physically transferring keys). For online transfers transaction costs are voluntary (typically 0.0001 BTC ~ 0.04 USD), and unrelated to the recipient and amount transferred. Units are fungible- every unit (or subunit) is equivalent and identical to any other.[72] Every unit is divisible up to 8 decimal places (As 1 dollar is 100 cents, 1 bitcoin is 100, 000, 000 satoshis.)

[70] Examples of web wallet services are: https://blockchain.info/wallet, http://mycelium.com/, https://www.coinbase.com/, https://www.elliptic.co/vault

[71] Wilber, D. Q., 'Woman With Printer Shows the Digital Ease of Bogus Cash', *Bloomberg*, 2014, (accessed 20 October 2014), http://www.bloomberg.com/news/2014-05-07/mom-with-hp-printer-shows-the-digital-ease-of-bogus-cash.html

[72] (accessed 25 October 2014). http://www.coindesk.com/bitcoin-fungibility-essential/

Users can acquire bitcoin through mining, purchasing bitcoin from other users through on bitcoin exchange, or by simply accepting bitcoin as payment for goods or services. However, mining has become a highly competitive affair and to enter to the market at this time would require significant investment in specialized bitcoin mining hardware.[73] The most common way to buy or sell bitcoins is through online bitcoin exchanges. There are currently 135 exchanges listed on the bitcoin wiki and facilitates bitcoin trading worldwide.[74] Using publicly posted prices and order books, bitcoin exchanges match customer orders directly and anonymously via automated algorithms. Bitcoin exchanges function similarly to stock exchanges, but different in the sense that users trade directly with one another and not through intermediary specialists as on NASDAQ or the New York Stock Exchange.[75] Another increasingly popular way of acquiring bitcoins is through a bitcoin ATM.[76]

Figure 3 – Bitcoin ATM Map by CoinDesk.com

Source: http://www.coindesk.com/bitcoin-atm-map/

3.3.3 A bitcoin Transaction

This section will describe the main steps of a bitcoin transaction by following a basic transaction between Alice the miner and Bob the merchant, from the moment of the decision to transfer the bitcoin, to the moment the network confirms the transaction.

[73] The network hashrate today is ~260,716,255 GH/s. If a miner were to decide to enter the market with enough computing power to have a 1 percent chance to solve the next block, the specialized hardware alone would cost approximately $ 2 million US$. (Not mentioning electricity costs).

[74] 'Exchanges'.(accessed 26 October 2014). https://en.bitcoin.it/wiki/Exchanges

[75] Lo, S. Wang, J. C. 'Bitcoin as Money?'. *Current Policy Perspectives, Federal Reserve Bank of Boston No 14-4.* 2014. pp 13.

[76] CoinDesk. 'Bitcoin ATM Map'. (accessed 26 October 2014). http://www.coindesk.com/bitcoin-atm-map/

Alice verified the last block and the network rewarded her with 25.5 BTC (25 new bitcoins and 0.5 in transaction fees from the block). Alice wants to buy more mining hardware from Bob, an online merchant selling the newest ASIC mining hardware. The new mining rig costs 5 BTC. Alice decides to purchase the new rig, and to add a transaction fee of 0.0001BTC.

Step 1 : Creating the Transaction

A transaction consists of inputs and outputs. The inputs are the address from which bitcoin will be sent and the outputs the addresses that will receive the bitcoin. The inputs and outputs are not necessarily equal; the difference being the transaction fees offered to the miner that verifies the transaction.

Antonopolous (2014) equates a transaction to a paper cheque: "Like a cheque, a transaction is an instrument that expresses the intent to transfer money and is not visible to the financial system until it is submitted for execution. […]While a cheque references a specific account as the source of the funds, a bitcoin transaction references a specific previous transaction as its source, rather than an account."[77]

Alice creates a transaction with the input as her address that contains 25.5 BTC, and the outputs are 5 BTC to Bob, 20.4999 to Alice (the 'change' from the transaction). The difference is 0.0001 and this is included as a miner's fee. After Alice created the transaction, she signs the transaction by encrypting it with her private key. This way anyone with Alice's public key can decrypt the transaction message, and verify that it was created by Alice. The transaction is now ready is now ready to be submitted for execution.

Step 2: Broadcasting the Transaction to the Network

Alice broadcasts the signed transaction to any node in the peer-to-peer network for verification. The node will validate that the inputs Alice used, are recognized previous outputs, and if valid, that node will broadcast the message to 3 – 4 nodes (each of which will independently validate the transaction and broadcast it to a further 3-4 nodes). Transactions with invalid inputs will never be rebroadcasted by the initial receiving node, and valid transaction will propagate in an exponentially expanding ripple across the entire network within seconds.[78]

---

[77] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies,* .O'Reily Media, 2014, (accessed 14 October 2014). http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#tx_bcast

[78] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies.* .O'Reily Media, 2014. (accessed 14 October 2014). http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#tx_bcast

Step 3: The Transaction is Included in a Block and Added to the Block Chain

After validating the transaction inputs, miners include the transaction in a block with other valid transactions coupled with demonstrated computational efforts through Proof-of-Work. Once a miner successfully verifies the block containing Alice's transaction, the miner is announces its find to the rest of the network. The other miners verify the validity of the new block, updates their versions of the global public ledger, and starts working of the next block. From this moment onwards, Bob is able to use the 5 BTC transaction output created by Alice, as an input in a new transaction.

3.4 The Current Economic State of Bitcoin (October 2014)

There are currently 13.5 million bitcoins in circulation, each valued at approximately 355 USD. Bitcoin is used in and the number of transactions per day ranges between 70,000 and 80,000. To put this into perspective: PayPal processes approximately 9.7 million transactions per day and Visa averages 150 million transactions per day.[79]

The price of bitcoin has been volatile. The first time a bitcoin traded for more than one USD was in April 2011. The price peaked in December 2013 at 1150 USD and throughout 2014 followed an overall downward trend with large fluctuations. Figure 4 shows the daily price variances of bitcoins and sterling expressed in terms of U.S. dollar.[80] While this comparison is a bit like comparing apples and oranges, this graph does indicate that the volatility of bitcoin is decreasing over time.

The Bank of England attributes Bitcoins price volatility mainly to the predetermined rate of supply and the fixed total supply. Since aggregate demand for money is volatile due to seasonal (Christmas shopping), cyclical (recessions) or structural (technological improvements) reasons, a money supply that is unable to respond accordingly will necessarily result in price volatility.[81]

---

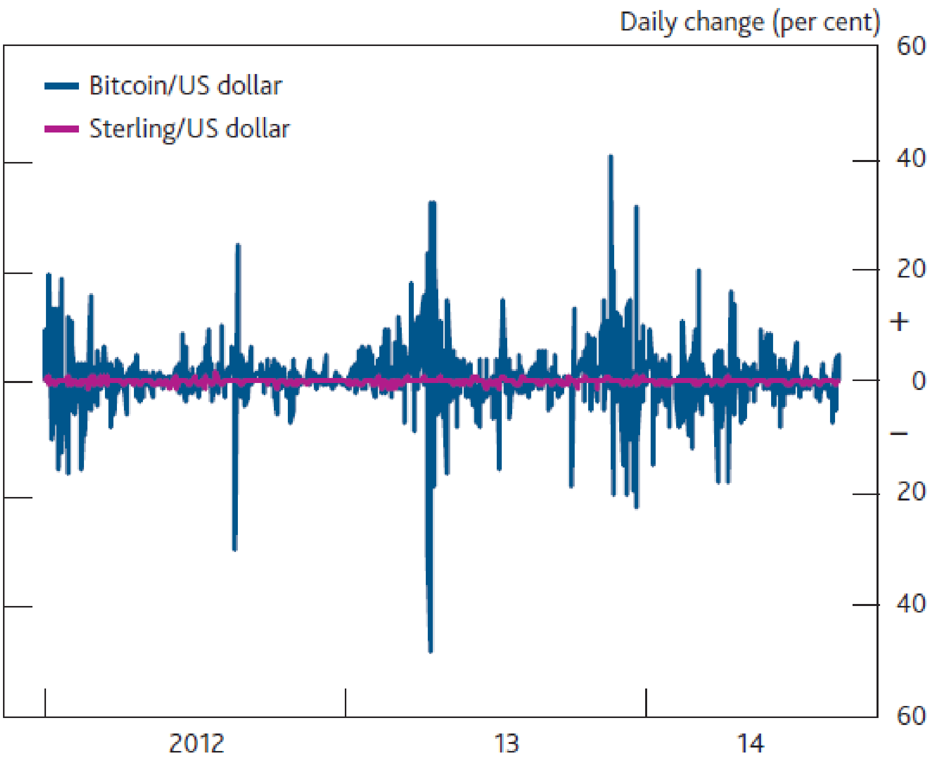
[79]Official webpages of Visa an Paypal, 2014, (accessed 25 October 2014)
http://usa.visa.com/merchants/industry-solutions/retail-visa-acceptance.jsp
https://www.paypal-media.com/about

[80] Ali, R. Barrdear, J. Clews, R. Southgate, J., 'The economics of digital currencies', *Bank of England Quarterly Bulletin2014 Q3,* 2014, (accessed 5 October 2014),
http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf

[81] Ali, R. Barrdear, J. Clews, R. Southgate, J., 'The economics of digital currencies. *Bank of England Quarterly Bulletin2014 Q3,* 2014, (accessed 5 October 2014),

In a report issued by CoinDesk, 'State of Bitcoin Q3 2014', more positive statistics are shown regardless of the deterioration in price. For the period September 2013 to September 2014 the report showed the following: Merchants accepting bitcoin as a means of payment increased eightfold and now totals 76 000; The number of unique bitcoin addresses increased threefold and now totals 184,554; All time venture capitalist investment into bitcoin related firms increased tenfold and now totals $317 million; The Network Hash Rate (computational power securing the network) has increased 216-fold.[82]

Figure 4: Bitcoin Price Volatility Compared to Sterling



Source: Bank of England Quarterly Bulletin 2014 Q3.

The majority of merchants accept bitcoin exclusively as a means of exchange, and not as a unit of account (prices are USD converted to BTC) of a store of value (does not keep the payment in bitcoin form). Merchants typically accept bitcoin through payment processors such as BitPay or Coinbase, which handles and stores bitcoins on their behalf. Bitcoin

http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf

[82] 'State of Bitcoin Q3 2014', CoinDesk, 2014, (Accessed 20 October 2014). http://www.slideshare.net/CoinDesk/state-of-bitcoin-q3-2014?qid=a856ddfe-f3e9-4f61-8fa1-b60ba2340d19&v=qf1&b=&from_search=1

payment processors also assume the volatility risk by offering merchants the option of immediate conversion of the bitcoin received into their local currency.[83]

4. The Benefits of Using Bitcoin as a payment system

The question is why anyone would want to use Bitcoin as a payment system instead of Visa or PayPal which are already commonly accepted.

As Bitcoin handles tasks usually entrusted to a central authority (verification of transactions, security of the system and regulation of the money supply) in a way that has never been used, the use of bitcoins as a means of exchange is radically different than everything that came before it. Its decentralized design grants users access to a payment system with no single point of failure. The network will process transactions unless all miners are forced to shut down their operations at once, this is a practical impossibility. In the absence of an intermediary to transactions, no mechanism for censorship or control exists. Anyone can easily create a Bitcoin address through which funds can instantly be received, and user's accounts cannot be "frozen". After a few confirmations, transactions are irreversible, and the only the holder of the private key of the receiving address has control over the coins.

The benefits to using Bitcoin as a payment system are economic (lower transaction costs, no cost of entry), practical (irreversible transactions in reasonably shot periods of time, geographical factors play no role) and conceptual (such as financial inclusion, censorship resistant). The following section will consider these benefits as they apply to different actors.

4.1 Economic Benefits

Due to the absence of an intermediary, Bitcoin transaction fees are generally significantly lower than that of other payment systems. Transaction fees are voluntarily added by the person initiating the transaction and the typical transaction fee is currently 0.0001 BTC (about 0.04 USD), regardless of the amount of the value being transferred, and regardless of the recipient. This contrasts against most payment systems, which usually charge a percentage of the transferred amount. Other economic benefits are that the acquisition of a Bitcoin address is free and instant; transaction processing time is 10 minutes on average; and that payments are irreversible.

[83] (accessed 25 October 2014). https://bitpay.com/features

Bitcoin can benefit merchants in several ways. For merchants, this process of setting up a Bitcoin address contrasts against the process for setting up an account with credit card payment systems like Visa or Mastercard. In order to accept credit and debit card payments, merchants must first obtain a merchant account by entering into an agreement with a member bank that has a processing relationship with Visa or Mastercard.[84] This agreement binds the merchant to the operating regulations as determined by the credit card company. Prior to the merchant account being granted, a merchant is subject to a comprehensive review of its business model and financial details, and smaller business owners must disclose their personal information and undergo a credit check.[85] The merchant account provider typically charges two fees per transaction: A per item flat rate as well as a percentage fee based on the total amount of the transaction (typically 2% to 5%). Merchants accepting credit card are also subject to chargebacks (the transaction is reversed) in cases where the card holder disputes a transaction on any ground (claims that card was stolen or that the merchant delivered unsatisfactorily).[86] Now consider a merchant accepting Bitcoin as payment: zero fees for creating a Bitcoin address, zero fees for accepting Bitcoin payments and zero risks of chargebacks.

Merchants thus not only benefit from lowered transaction costs, but also the reduced fraud risk. The Chairman of a large U.S. online retailer Overstock emphasizes that of the reduced fraud risks when using Bitcoin is benefits both merchant and customer:

> One, the merchant who is accepting bitcoin doesn't hold any meaningful personal identifiable information about the customer. If you purchase something on our site with bitcoins, yes you give us a shipping address, but you don't give us a credit card number or bank account details. On the off-chance someone hacked into our site, there is nothing there to target and steal. Two, we spend a lot of money and effort on fraud prevention, stopping the use of stolen credit cards, but we don't have to worry about that fraud prevention effort with bitcoin because there is no charge-back available.[87]

---

[84] 'How to Set Up a Merchant Account'. 2011. (Acessed 10 October 2014). http://paysimple.com/blog/2011/09/07/how-to-set-up-a-merchant-account/

[85] *Ibid.*

[86] Conde, J. 'Merchant Accounts 101'. 2013. (accessed 10 October 2014). http://www.merchant-account-services.org/article/merchant-accounts-101/11

[87] Wright, G., 'Is bitcoin good for business?', *Global Finance, 28*(6). 2014. (accessed 10 October). http://bitcoinchamberofcommerce.com/?p=448

Overstock started accepting bitcoins as payment in January 2014. In a statement to Reuters during August 2014, the CEO said Overstock has processed more $2 million worth or transactions in bitcoin, and expects total bitcoin sales of $6 million to $8 million in 2014.[88]

Lower transaction costs also allow micro-payments, giving businesses the opportunity to monetize low-cost goods or services sold online, which current transaction costs make unfeasible. For example a user could pay for a single song instead of purchasing an entire album, or pay to read a single article on a news-site instead of purchasing a monthly subscription.

There are also potential beneficiaries are on the other side of the financial spectrum: The “unbanked” and the international migrant remittances market.

4.2 Financial Inclusion

Financial inclusion of the unbanked and the state of the international remittances market form the focus of the 2014 Global Financial Development Report released by the World Bank.[89] This report emphasizes the importance of financial inclusion for economic and social development.[90] The World Bank states that there is a growing worldwide recognition “that access to financial services has a critical role in reducing extreme poverty, boosting shared prosperity, and supporting inclusive and sustainable development.”[91] So who are the unbanked? According to the report, approximately 50 percent of adults (2.5 billion) without access to a basic bank account, and while some have no demand for accounts, most are excluded due to barriers such as cost, distances, documentation requirement regulations or a

---

[88] Chavez-Dreyfuss, G., ‘Exclusive: Overstock CEO says bitcoin sales to add 4 cents to 2014 EPS’. 2014. (Accessed 14 October 2014). http://www.reuters.com/article/2014/08/13/us-overstock-com-bitcoin-idUSKBN0GD21220140813

[89] World Bank,’Financial Inclusion’, Global Financial Development Report, 2014. pp 21. (accessed 14 October 2014). http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTGLOBALFINREPORT/0,,contentMDK:23489619~pagePK:64168182~piPK:64168060~theSitePK:8816097,00.html

[90] World Bank,.’Financial Inclusion’. *Global Financial Development Report 2014*. pp 21. (accessed 14 October 2014), http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTGLOBALFINREPORT/0,,contentMDK:23489619~pagePK:64168182~piPK:64168060~theSitePK:8816097,00.html

[91] *Ibid.*

lack of trust in banks.[92] In the developing world, fixed transaction cost and annual fees make tend to make small transactions unaffordable. For example, total annual fees on a checking account in Sierra Leone are equivalent to 27 percent of GDP per capita.[93] High costs associated with opening and maintaining accounts in small developing countries are identified as a consequence of the lack of competition and underdeveloped physical or institutional infrastructures. The lack of bank branch penetration also explains the distance as being a major reason for exclusion. In Tanzania, 47 percent of the unbanked cite distance as the primary reason.[94] In Europe and Central Asia, 31 percent of the unbanked cite distrust in banks as a reason. Distrust can stem from “discrimination against certain segments of the population, past episodes of government expropriation of banks, or economic crises and uncertainty.”[95]

Remittances are among the most important financial transactions for the populations that have limited access to formal banking services. The World Bank (2014) estimates that officially recorded international migrant remittances to developing countries totaled $401 billion. In 2012 the global average cost of remittance transactions was 8 percent of the amount transferred. While some countries enjoy lower fees, those who need it most are above. Approximately $60 billion in remittances was sent to the African continent in 2012, with an average cost per transaction of 11.89 percent. However, the more alarming part of this statistic is that transaction cost actually increased from 10.90 percent in 2011.[96]

The World Bank (2014) states: “Given the potential role of remittances in raising financial inclusion, it is important to make transfer systems less costly, more efficient, and more transparent.”[97] Furthermore, the World Bank recognizes that technological innovations are able to make it easier and less expensive for people to use financial services, while increasing financial security. The technological innovations already exist to allow anyone with a mobile

[92] *Ibid*, pp. 34.

[93] *Ibid*, pp. 54.

[94] *Ibid*, pp. 55. Bank penetration in Tanzania averages less than 0.5 bank branches per 1,000 square kilometres.

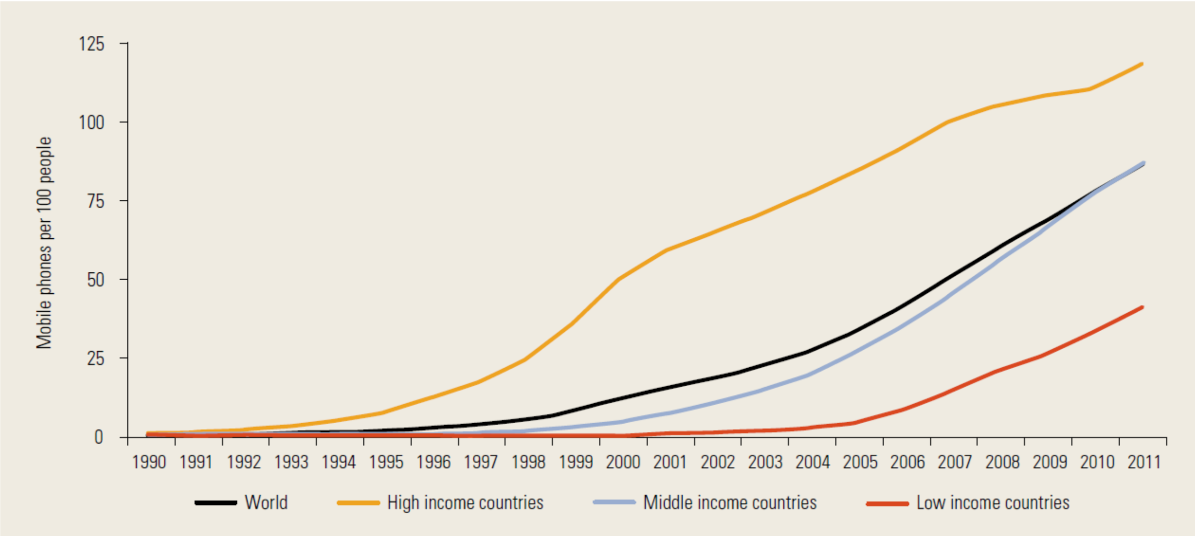
[95] *Ibid*, pp. 55.

[96] Cirasino, M., ‘How can we cut the high costs of remittances to Africa’, *World Bank Blog*, 2013., (Accessed 20 October 2014), http://blogs.worldbank.org/psd/how-can-we-cut-the-high-costs-of-remittances-to-africa

[97] World Bank, ’Financial Inclusion’, *Global Financial Development Report 2014*, 2014. pp 76, (Accessed 14 October 2014), http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTGLOBALFINREPORT/0,,contentMDK:23489619~pagePK:64168182~piPK:64168060~theSitePK:8816097,00.html

phone to utilize innovative payment systems such as Bitcoin. Fig. 2 shows the rapid increase of mobile phone technology adoption in the developing world.

Figure 2: Mobile Phones per 100 People, by Country Income Group, 1990–2011[98]



Source: World Development Indicators (database), World Bank, Washington, DC, http://data.worldbank.org/data-catalog/world-development-indicators.

Fig. 2 suggests that the developing world's unbanked and remittance paying migrants may be ripe for conceptual and economic benefits associated with innovative new payment systems. To harness the promise of new technologies, regulators need to allow competing financial service providers and consumers to take advantage of technological innovations . The World Bank states that regulators must ensure that "first, new technologies are adopted and, second, that they are priced and made available in a way that makes them accessible to the unbanked" by creating a regulatory framework which "create enabling conditions for the providers of technology-based financial services, while protecting the rights of consumers."[99]

5. Risks

There are many risks involved in the use of virtual currency schemes and most central authorities have issued warning statements regarding risks of use and speculation of bitcoin. This section will describe the risks involved for users, risks to financial integrity and risks to regulators.

[98] *Ibid.* pp 54.

[99] World Bank.'Financial Inclusion', *Global Financial Development Report 2014*, 2014. pp 76. (Acessed online 14 October) http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTGLOBALFINREPORT/0,,contentMDK:23489619~pagePK:64168182~piPK:64168060~theSitePK:8816097,00.html

5.1 Risks to Users

In the absence of a central authority or intermediary, users of virtual currency enjoy less consumer protection than typically afforded by traditional banking and payment services. Bitcoin users are exposed to risks of theft or fraud, and price volatility. While Bitcoin is designed to function as a decentralized system that does not require users to trust or depend on third parties, in practice users often trust third parties such as exchange operators and wallet service providers to not act fraudulently and to have sufficient security safeguarding their systems.

Users that personally store their keys have the risk of permanently losing their funds if they lose their passwords/private key or if their hard drive containing their wallet crashes without having a backup. In this case the funds will be stuck in that address and can never be retrieved. Users also risk permanently losing their funds if their computer becomes infected with malicious software that steals their private keys. In the event of loss or theft, no recourse is available, since there is no central authority.

Users entrusting third party service providers such as exchanges or web wallet providers with their funds, risk loss as a result of fraudulent actors or pure mismanagement. Most companies built around virtual currencies are to be considered as startups which operate in unsure regulatory space. Startup companies have massive potential, but are also at high risk of mismanagement or even fraud, and thus failure. Many (if not most) exchanges have failed, and large amounts of users' funds have been lost. The most famous case is that of Mt.Gox, a Bitcoin exchange based in Tokyo, Japan. In February 2014 Mt. Gox, the largest and longest operating bitcoin exchange at the time, stopped trading and filed for bankruptcy after discovering that as many as 650,000 bitcoins (worth approximately US$465 million at the time) had been lost due to a security breach.[100] The Bitcoin community remains skeptical and many are of the opinion that the loss was due to gross negligence or even internal theft. In response to the failure of Mt. Gox, the Bitcoin Foundation stated: "This is certainly not the end of Bitcoin. As our industry matures, we are seeing a second wave of capable, responsible entrepreneurs and investors who are building reliable services for this ecosystem."[101] And indeed today the situation is different. The number of identifiably trustworthy actors has increased significantly. One example is Circle Internet Financial Inc. which is backed by

[100] 'Hackers hit web accounts of MtGox boss', *BBC Technology News*, 2014. (Accessed 20 October 2014). http://www.bbc.com/news/technology-26387800

[101] 'Bitcoin - Turbulent Waters - Part Seven', *Dorsey & Whitney LLP*, 2014. (Accessed 20 October 2014), http://www.dorsey.com/eu_cm_bitcoin_virtual_currency_pt7/

US$26 million in venture capital investment and boasts with a respectable management board. Circle Internet Financial allows customers to use credit cards to purchase bitcoins, provides a secure platform for users to send bitcoins to each other, and most unique in the Bitcoin ecosystem, all clients' funds stored on their system are fully insured at zero cost.[102]

When using bitcoins as a means of payment, there is little protection for the customer in the event that the counterparty fails to meet his contractual obligations. While merchants view chargebacks as a disadvantage, this measure of consumer protection is unavailable to users paying in bitcoin since there is no intermediary to appeal to. Thus, when making payments, users have more responsibility to verify the authenticity of the counterparty, as well as being more diligent in executing the transaction correctly. In the event of transferring bitcoins to a malicious party, or transferring bitcoins to an incorrect address, there is no recourse and the funds are lost.[103]

Users invested in Bitcoin are exposed to significant price volatility. The price of bitcoin experiences large and sudden fluctuations due to many factors which are generally uncontrollable, such as the extent of adoption and future expectations. Furthermore, the market depth is low, large buy/sell orders on exchanges cause noticeable fluctuations in the exchange rate.[104] The lack of a central bank combined with a fixed rate of supply is criticized by economists citing the need for macro-economic stabilization. Within the Bitcoin system, counter cyclical inflationary stimulus is impossible, and thus changes in demand for money will result in changes the price.[105]

Another risk faced by users is the possibility of Bitcoin losing all value if the network consensus is undermined. The existence Bitcoin's value relies on the uncompromised functioning of the protocol, and users' confidence that the network will remain functioning. Bitcoin's functioning could be compromised by '51% attack'- if the majority of the network's computational power is controlled by a malicious actor. If a single miner (or a pool of miners), controls the majority of the network's processing power it would be able to alter the current consensus over the rules of the network and could enable double spending or prevent

[102] Circle Financial Inc. website, 2014, (accessed 25 October 2014), https://www.circle.com/en

[103] European Central Bank. 'EBA Opinion on 'virtual currencies'. 2014. *EBA/Op/2014/08*. pp 23.

[104] *Ibid.*

[105] Dourado, E & Brito, J., 'Cryptocurrency, 'The New Palgrave Dictionary of Economics', Eds. Steven N. Durlauf and Lawrence E. Blume, Palgrave Macmillan, 2014, *The New Palgrave Dictionary of Economics Online*, Palgrave Macmillan. 20 October 2014. (accessed 20 October 2014). http://www.dictionaryofeconomics.com/article?id=pde2014_C000625

transactions from being included in blocks.[106] Bitcoin is designed that a 51% attack should never happen, since a profit seeking miner will always gain more by following the rules – by regularly solving blocks and receiving new bitcoins and transaction fees. If a 51% attack would be executed, it could destroy trust in the functioning of the network and which would nullify any proceeds attained through double spending. However, attackers might not be financially motivated and might attack the network for reasons outside the Bitcoin economy. An attacker controlling with 51% of the networks processing power could extend the block chain with empty blocks, and prevent any transactions from being confirmed. While honest miners (the 49%) will also find blocks, the attacker will simply keep extending his private version of the block chain which will eventually be longer than the honest block chain. When the attacker then eventually broadcasts its longer block chain, it will replace all blocks since the start of the attack with blocks excluding some (or all) transactions. This would result in some (or all) transactions that were confirmed during the attack, becoming unconfirmed. While these attacks could theoretically happen, the proceeds from the attack would never justify the immense investment required to perform it.[107]

5.2 Risks to Financial Integrity

Risks to financial integrity refer to exploitation of the pseudonymous nature of users and the borderless nature of the payment system.[108] Since addresses are not directly linked to individual identities, the system has the potential to be used for money laundering, terrorist financing and other financial crimes.[109]

The risk of facilitating money laundering and terrorist financing arises as Bitcoin transactions are carried out on peer-to-peer basis between parties without any identification requirements. Anti-money-laundering (AML) efforts face a more elusive target as it is not only more difficult to determine the identities of parties to a transaction, but the transaction itself is also unable to be interrupted. [110] While all transactions publicly recorded in block chain, the

[106] 'Weaknesses', 2014, (accessed 20 October 2014), https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

[107] Trautman, L., 'Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law & Technology. Volume XX(4),* 2014, pp 56. (accessed 28 October 2014). http://jolt.richmond.edu/v20i4/article13.pdf.

[108] European Central Bank, 'EBA Opinion on 'virtual currencies', 2014. *EBA/Op/2014/08*. pp 32.

[109] *Ibid*. pp 32.

[110] Bryans, D., 'Bitcoin and Money Laundering: Mining for an Effective Solution', *Indiana Law Journal Vol. 89:441*, 2014, pp 445.

existence of bitcoin mixing services allow users to maintain anonymity if they want to. Bitcoin mixers provide services that obscure the flow of bitcoins from one address to the next, by mixing the large amounts of bitcoins through many transactions, and returning clean bitcoins to the user. Bryans (2014) states that Bitcoin could enable money launderers to "move illicit funds faster, cheaper, and more discretely than ever before."[111]

The anonymity afforded to users coupled with zero entry costs makes Bitcoin attractive for criminals as a means of payment for illegal commodities and services via hidden online marketplaces called "dark markets". Dark markets, similar to eBay, provide an infrastructure for sellers and buyers to trade over the internet. Dark markets are not accessible through normal internet browsers, but require the use of TOR ("The Onion Router") which conceals true IP addresses and thus the identities of the network participants.[112] Most vendors on these marketplaces only accept Bitcoin as payments, and some marketplaces even have automatic mixing services to ensure the anonymity of parties to each transaction. One such marketplace, called the Silk Road, was shut down in October 2013 by the FBI. Prior to being shut down, the Silk Road website was visited by hundreds of thousands of unique users from countries across the globe on a daily basis.[113] In September 2013, the website had approximately 13,000 listings of illegal goods (such as illegal substances, counterfeit US dollars, forged passports, weapons) and services (such as computer hacking and even assassinations).[114] The only form of payment that was accepted on Silk Road was bitcoins, and sellers would use the normal postage system to deliver goods. During the site's two and a half year existence, it facilitated illegal trades valuing roughly $1.2 billion, and generated $80 million in commissions. The FBI arrested the alleged creator of Silk Road, Ross Ulbricht, and seized his laptop which contained 144,336 bitcoins. A further 29,655 bitcoins were seized from a servers which were used to run the Silk Road website.[115] In July 2014, the U.S. Marshals auctioned off the 29,665 bitcoins (valued at approximately $17 million) in a public auction, with the winning bid from

---

[111] Bryans, D., 'Bitcoin and Money Laundering: Mining for an Effective Solution', *Indiana Law Journal Vol. 89:441*, 2014, pp 447.

[112] Ron, D. Shamir, A., 'How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?', *Department of Computer Science and Applied Mathematics, The Weizmann Institute of Science, Israel,* 2013, pp. 1.

[113] *Ibid.*

[114] *Ibid.*

[115] Hern, A., 'US government prepares to auction $17m of seized Silk Road bitcoins', *The Guardian.* 2014. (Accessed 24 Octber 2014), http://www.theguardian.com/technology/2014/jun/24/us-auction-seized-silk-road-bitcoins

venture capitalist Tim Draper.[116] The auction is indicative that the U.S. recognizes the legality of Bitcoin. The remaining 144,336 bitcoins are still held by the authorities pending the outcome of the Ulbricht's trial which starts in January 2015.[117]

In the six months following the shut-down of Silk Road, new dark markets proliferated and the number of illicit goods and services listings totaled more than 32,000 by March 2014, almost triple the listings found on Silk Road in 2013.[118]

Previous virtual currencies used for illicit transactions have been shut down by the U.S. Department of Justice. The first was E-Gold, which operated within the U.S., and more recently Liberty Dollar, which was incorporated in Costa Rica. E-gold, founded in 1996, was a centralized virtual currency which was backed by precious metals. Before it was shut down it had more than $60 million dollars in deposits and more than 4 million user accounts. E-gold allowed users to create accounts without any identification requirements, and soon became a mechanism used by criminals for illicit transactions and money laundering.[119] In 2008 e-gold and its three directors pleaded guilty to charges of "conspiracy to engage in money laundering and the "operation of an unlicensed money transmitting business".[120] After the failure of E-Gold and the criminal conviction of those involved, defendant Arthur Budovsky immigrated to Costa Rica and incorporated Liberty Reserve, a payment system specifically designed to "succeed in eluding law enforcement outside the U.S."[121] Liberty Reserve was shut down in 2013 on the grounds that it facilitated money laundering in excess of $6 billion during its existence. Liberty Reserve required account holders to declare their

---

[116] Silk Road Bitcoin Auction Winner Tim Draper Won't Say How Many Millions He Paid. *Forbes*, 2014, (accessed 25 October 2014), http://www.forbes.com/sites/kashmirhill/2014/07/02/tim-draper-silk-road-bitcoin-auction/

[117] The funds are held in the following address: https://blockchain.info/address/1i7cZdoE9NcHSdAL5eGjmTJbBVqeQDwgw

[118] Wong, J. I., 'Dark Markets Grow Bigger and Bolder in Year Since Silk Road Bust', CoinDesk, 2014, (accessed 20 October 2014), http://www.coindesk.com/dark-markets-grow-bigger-bolder-year-since-silk-road-bust/

[119] Foley, S. 'Bitcoin needs to learn from past e-currency failures'. *The Financial Times.* 2014. (accessed 25 October 2014). http://www.ft.com/cms/s/2/6d51117e-5806-11e3-a2ed-00144feabdc0.html

[120] Wenzel, R. 'Bitcoiners: Remember What Happened to eGold'. *Economic Policy Journal.* 2013. (accessed 24 October 2014). http://www.economicpolicyjournal.com/2013/04/bitcoiners-remember-what-happened-to.html

[121] Trautman, L., 'Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?', *Richmond Journal of Law & Technology Volume XX(4)*, 2014, pp 86, (accessed 28 October 2014). http://jolt.richmond.edu/v20i4/article13.pdf,

identity, address and birth date, yet did not require any documentation to support these declarations, and the content of the declaration had no effect on the validity of the account.[122]

Decentralized virtual currencies like Bitcoin present difficult law enforcement challenges since no central point can be targeted, and it is impossible to regulate the system itself and enforce obligatory registration or know your customer procedures. The online drug trade industry is developing at a rapid pace and presents new enforcement difficulties. James Martin(2014), a drugs trade researcher states:

> "With online drug trading, you have hidden financial transactions; the dealer and customer never meet in the same place; you have drugs arriving in the post [...] all of this breaks the 'business model' of conventional law enforcement."[123]

5.3 Risk to regulators

This section addresses the risks faced by regulatory authorities. At this early point in the existence of decentralized virtual currencies, most authorities regulate its use under existing legislation as either a currency or as an asset, depending on whether it is used as a means of exchange or as a speculative investment. If the acceptance of decentralized virtual currencies increase and amount to a greater economic significance, specific legislation and perhaps new regulatory bodies might be needed on account of the unique nature of these virtual currencies. Regulators face reputational risks, and risks regarding the competitive objectives within the economy.

Regulatory authorities face reputational risks. If the chosen regulatory response is ineffective the credibility of the regulators would be undermined. In the event of under-regulation, the risks faced by users and the threats to financial integrity would be unmitigated. Since virtual currencies offer the same services as traditional payment systems while falling outside current regulations applicable to payment systems, the regulators objective of ensuring well-functioning payment systems is undermined. [124]

In the case of over-regulation, states risk driving away technological innovation and the economic activity to other countries, given Bitcoin's borderless nature. It must be understood that Bitcoin is a protocol on which a currency is able to function, just as HTTP is the Internet protocol on which email is able to function. It is impossible to predict all future applications

[122] *Ibid.*

[123] *Ibid.*

[124] European Central Bank, 'EBA Opinion on 'virtual currencies'. *2014. EBA/Op/2014/08*. pp 36.

of the Bitcoin protocol or different implementations of block chain technology at this point in its development, just as it was impossible to predict all future applications of the internet in 1994.

5.4 Risk of undermining the State´s monopoly on currency.

In modern states using fiat currency systems, the state exerts control over the money supply and uses it to steer the economy and control inflation. Through central banks, states are able to actively strengthen and stabilize the economy through promoting employment, stable prices, and moderate long-term interest rates.[125] To effectively pursue these goals, Central banks require a high degree of control over the currency. The central banking institution exerts control over the money supply mainly through open market operations. Open market operations as the dominant form of monetary policy, refers to the central bank´s participation in the market for government bonds. By buying or selling bonds in the public market, the central bank is able to expand or contract the money supply, which influences the federal funds rate (the interest rate applicable on short term interbank loans). Changes in the federal funds rate has a cascading effect on the economy by influencing general interest rates.[126] Lower interest rates make borrowing money cheaper and saving money less profitable, and thus encourages borrowing over saving. Increased borrowing equates to increased spending and thus, increased economic activity. With lower interest rates, more money enters circulation, increasing economic growth and leads to an increased rate of inflation. A central bank aims to maintain a low, positive rate of inflation in order to discourage holding on to money. With a positive rate of inflation, money loses purchasing power over time and people are encouraged to spend and invest their money in order to increase (or at least maintain) their purchasing power. The state´s monopoly over the creation money is essential to this process, and competing or alternative currencies could undermine the effectivity of central banks.[127]

The existence and adoption of competing currencies undermines the powers of the state by creating doubt in the value of the fiat currency. This suggests the concern that competing currencies devalue the currency of the state, a process which is difficult to stop once it gains momentum.[128] States thus have an incentive to prevent competitive currencies.

---

[125] Cook, R. J., ´Bitcoins: Technological innovation or Emerging Threat?´. *The John Marshall Journal of Information Technology and Privacy Law. Volume 30(3) 535.(*2014), pp 550.

[126] *Ibid.*

[127] *Ibid.*

[128] Cook, R. J., ´Bitcoins: Technological innovation or Emerging Threat?´, *The John Marshall Journal of Information Technology and Privacy Law. Volume 30(3) 535*, 2014, pp 544.

An example of the state responding to a competing currency is the case of the Liberty Dollar in the U.S, a private commodity currency. A man named Bernard von NotHaus established the National Organization for the Repeal of the Federal Reserve and International Revenue Code (NORFED). NORFED aimed to circulate a commodity currency to serve as an alternative to the U.S. dollar called the Liberty Dollar, a private currency backed by precious metals which was launched in 1998. The purpose was to create an inflation-proof currency, which retains its purchasing power over time. As the price of silver increases over time the value of the currency increases, as opposed to fiat currency which loses value over time. The Liberty Dollar was shut down when Von NotHaus was charged for counterfeiting (due to similarities between the Liberty Dollar and the U.S dollar) in addition to charges under the U.S anti-competitive currency statute, 18 U.S.C. §486.[129] Von NotHaus was charged and convicted (2011), in part, due to his intention to compete with the U.S. dollar by circulating Liberty Dollars as if they were U.S. dollars.[130] At that time there was roughly $20 million Liberty Dollars in circulation.

When people turn to alternative currencies as a store of value instead of the local fiat currency, it reduces the overall demand for fiat currency, and thus the central banking institutions´ ability to stimulate demand.[131] If Bitcoin gains widespread adoption, it could pose a risk to the central banking institutions’ ability to influence demand, and without a central authority to hold accountable or shut down, it is unclear what could be done in such a case.[132]

[129] Cook, R. J., ´Bitcoins: Technological innovation or Emerging Threat?´, *The John Marshall Journal of Information Technology and Privacy Law. Volume 30(3) 535*, 2014, pp 548.

[130] *Ibid.*

[131] Cook, R. J., ´Bitcoins: Technological innovation or Emerging Threat?´,*The John Marshall Journal of Information Technology and Privacy Law. Volume 30(3) 535*, 2014, pp 548.

[132] *Ibid.*

6. Regulation of Virtual Currencies

Due to Bitcoin's decentralized structure, pseudonymous nature of its users, and irreversibility of transactions, effective regulation of this rapidly emerging technology requires a novel approach. As Bitcoin is not created or controlled by any central entity, regulations typically applicable to the banking and the financial industry may not be suitable for Bitcoin and Bitcoin transactions.[133]

Regulators lack the ability to impose regulatory requirements (or impose accountability) upon a centralized entity that could assist with detection and prevention of illicit activity. It is not feasible to regulate senders and receivers of bitcoin since there is no requirement to exchange personally identifiable (PII) when making transactions. The costs of attempting to track all users who have not provided any PII, largely outweighs the benefit of exposing minor transactions.[134] In the event of regulation targeting users directly, it might result in users not only using methods to attain even greater anonymity, but also could cause users to lose confidence in the regulators. More efficient points of regulation are the entities within the Bitcoin economy where users are concentrated such as exchanges and payment processors. Regulation of exchanges could be feasible under existing laws that apply to money transmitters. Money transmitters are required to implement AML and KYC procedures, and obtain necessary licenses and complete registration procedures prior to being able to lawfully conduct business.[135]

Member of the Executive Board of the European Central Bank, Mr. Yves Mersch(2014) stated that given the economic size of virtual currency schemes in Europe: "virtual currencies do not pose a risk to price stability or financial stability, but do pose a risk for users. However, this user risk is more related to speculative investments and consumer protection, and not necessarily to payments."[136] This statement encapsulates the idea that regulations of this new technology should focus on mitigating risks faced by users, and regulators should be

---

[133] Gilbert, R. N. & Blye A. D. 'Bitcoin and Internet Payment Systems: Regulatory and Commercial Law Concerns', *Carlton Fields Jorden Burt*, 2014, (accessed 30 September 2014), http://www.cfjblaw.com/bitcoin-internet-payment-systems-regulatory-and-commercial-law-concerns/#_edn15

[134] Bryans, D. 'Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal Vol. 89:441*. 2014. pp 472.

[135] Trautman, L. 'Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law & Technology Vol.XX:4.* 2014. (accessed 28 October 2014). http://jolt.richmond.edu/v20i4/article13.pdf. pp 24.

[136] Mersch, Y. 'Efficient retail payments - key in strengthening the competitiveness and growth potential of the EU'. 2014. (accessed 25 October 2014). http://www.bis.org/review/r140324a.htm

cautious to not stifle innovation and prevent the realization of the greater economic benefits (for 'the unbanked' and the global remittances market) associated with decentralized virtual currencies.

In a survey conducted by the U.S. Law Library of congress, 40 countries were requested to provide comments of their official stances on Bitcoin.[137] The comments addressed three primary themes: That Bitcoin does not have legal tender status, aspects of consumer protection, and clarification regarding taxation.[138] The status and regulation of Bitcoin in a few notable countries will be discussed below.

Most countries have indicated that there no immediate intention to implement regulation of Bitcoin at this point in time. Many countries (Singapore, U.K., Germany, will be briefly discussed below) have provided clarification regarding tax obligations arising from the use of Bitcoin and, classifying it as an asset if it is speculated upon, and as income if used as a means of payment, but have not made specific legislation.[139] Few countries (China, Russia and Brazil will be briefly discussed below) have implemented virtual currency specific legislation, either effectively banning Bitcoin, or actively promoting its development.[140] Most recently, the U.S. Financial Crimes Enforcement Network (FinCEN) has announced that all virtual currency exchanges and payment processors may be required to obtain money services businesses licenses under U.S. Law.

In Singapore, the financial services regulator, The Monetary Authority of Singapore (MAS), does not directly regulate or interfere with Bitcoin, since virtual currencies are not considered legal tender or securities under the Securities and futures Act.[141] The MAS recognizes the potential money laundering and terrorist financing risks and consequently regulates virtual currency intermediaries (Bitcoin exchange operators and Bitcoin ATM machines) that trade or facilitate the trade of virtual currencies for fiat currencies to verify the identification of customers and to report suspicious transactions to the Commercial Affairs Department

---

[137] 'Regulation of Bitcoin in Selected Jurisdictions', *The Law Library of Congress, Global Legal Research Center*, 2014, (accessed 10 October 2014), http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

[138] Shaheen, K., 'Regulation of Bitcoin around the world´. *Lexology, Dentons*,2014, (accessed 18 October 2014), http://www.lexology.com/library/detail.aspx?g=d92a33fe-3f11-43f6-b0cf-d8476ca612b1

[139] Shaheen, K., 'Regulation of Bitcoin around the world´. *Lexology, Dentons*.2014, (accessed 18 October 2014), http://www.lexology.com/library/detail.aspx?g=d92a33fe-3f11-43f6-b0cf-d8476ca612b1

[140] *Ibid*.

[141] Monetary Authority of Singapore, 'Reply to Parliamentary Question on Virtual Currencies', Notice Paper 62, 2014, (accessed 30 September 2014), http://www.mas.gov.sg/news-and-publications/parliamentary-replies/2014/reply-to-parliamentary-question-on-virtual-currencies.aspx

(effectively treating it as money).[142] Regarding taxation, The Inland Revenue Authority of Singapore (IRAS) states that virtual currency is not treated as currency or goods, but as a 'supply of services'. When users purchase goods or services with virtual currency, the IRAS considers the transaction a 'barter trade' with two suppliers, both of which are taxed as service suppliers.[143]

The United Kingdom announced that it will treat Bitcoins like any other form of payment for tax purposes: Value Added Tax will be due in the normal way from suppliers of any goods or services sold in exchange for Bitcoins. The Bank of England has released two comprehensive reports regarding virtual currencies in which it concludes that Bitcoin currently does not "pose a material risk to monetary and financial stability in the U.K." given the small size when compared to the sterling. [144]

The German Ministry of Finance treats the commercial sale of bitcoins as a sale of 'other services' (subject to VAT) and does not recognize it as currency, legal tender or e-money in terms of payment supervision legislation.[145] [146] When Bitcoin is used by individuals as a money substitute, the Federal Financial Supervisory Authority (BaFin) qualifies bitcoins as "*Rechnungseinheiten*" (legally binding financial instrument in the category of units of account) that serves as a private means of payment in barter transactions, regardless of not being denominated in legal tender.[147] Germany's Fidor bank has integrated a virtual currency

---

[142] Monetary Authority of Singapore, 'MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks', 2014, (accessed 30 September 2014), http://www.mas.gov.sg/news-and-publications/media-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.aspx

[143] Inland Revenue Authority of Singapore, 'GST treatment for e-Commerce transactions: Sale of virtual currency', 2014, (accessed 30 September 2014), http://www.iras.gov.sg/irashome/page04.aspx?id=2276

[144]'Digital currencies: Quarterly Bulletin 2014 Q3 pre-release articles'. 2014. (accessed 15 October 2014). http://www.bankofengland.co.uk/publications/Pages/quarterlybulletin/2014/qb14q3prereleasedigitalcurrenciesbitcoin.aspx

[145] 'German Ministry of Finance declares Bitcoin payments sales-taxable', *The Bundesverband Bitcoin, German affiliate of the Bitcoin Foundation* , 2014, (accessed 30 September 2014), http://www.bundesverband-bitcoin.de/?p=221

[146]Payment Services Supervision Act of 25 June 2009 (Federal Law Gazette 1, p. 1506), as amended by Article 2 subsection (74) of the Act of 22 December 2011 (Federal Law Gazette I, p. 3044)

[147] German Federal Financial Supervisory Authority, 'BaFin Annual Report 2013', 2014 , pp.58. (accessed 30 September 2014), http://www.bafin.de/SharedDocs/Downloads/EN/Jahresbericht/dl_annualreport_2013.pdf?__blob=publicationFile

called Ripple. Since September 2014, Fidor allows customers to complete international wire transfers via the Ripple protocol.[148]

Countries that have banned or severely regulated virtual currencies include Russia and China. The Russian Ministry of Finance announced a legislation initiative that would "recognize the act of engaging in Bitcoin transactions as a misdemeanor and impose fines for "transactions with a cybercurrency and creation and distribution of software used for the issuance of monetary surrogates" in an amount up to the equivalent of $30,000."[149] In China, Bitcoin is treated as a special virtual commodity, and banks and payment institutions are prohibited from dealing in Bitcoin or providing services which are directly or indirectly related to Bitcoin.[150]

On the other side of the spectrum some countries have taken step towards recognition and regulation of Bitcoin as a valid currency. Brazil enacted legislation in late 2013 which created the possibility "for the normalization of mobile payment systems and the creation of electronic currencies" which includes Bitcoin.[151] The Brazilian tax authority have announced that as a financial asset- bitcoin transactions are subject to capital gains tax, but only if capital gains exceed $15,000. Such a framework is effective in collecting taxes from investors, without obstructing the activities of bitcoins users that use it as a means of payment.[152]

In the U.S., Bitcoin is regarded as a currency without legal tender status by the Financial Crimes Enforcement Network (FinCEN). Regarding taxation: When Bitcoin is received as payment for goods or services, it forms part of general income and is subject to taxation. Miners rewards are includible in gross income, and thus also subject to income tax.[153] Bitcoins are also treated as an asset which is subject to capital gains tax, but there is no exemption threshold as under the Brazilian legislation. On 27 October, 2014, FinCEN

---

[148] Carney, M., 'German's Fidor bank will begin using Ripple for international wire transfers next week.' *Pando Daily*.http://pando.com/2014/08/22/germans-fidor-bank-will-begin-using-ripple-for-international-wire-transfers-next-week/.

Fidor Bank, 2014, https://www.fidor.de/faq/ripple

[149] 'Russia: Fines for Bitcoin Transactions Will Be Introduced'. (accessed 25 October 2014). http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205404151_text

[150] 'Regulation of Bitcoin in Selected Jurisdictions'. *The Law Library of Congress, Global Legal Research Center*. 2014. (accessed 10 October 2014). http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

[151] *Ibid.*

[152] De Filipi, P., 'Bitcoin: a regulatory nightmare to a libertarian dream'. *Internet Policy Review Vol. 3:2*. 2014. (accessed 20 October 2014), http://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream

[153] BitLegal. United States, 2014, (accessed 31 October 2014). http://bitlegal.io/nation/US.php

released new guidelines for Bitcoin related companies such as exchanges and payment processors.[154] The guidelines state that these companies may be considered money services businesses (MSB) under U.S. law. MSB must register with FinCEN to obtain money transmitter licenses, which are issued on a State level. This means that these companies must acquire a money transmitter license, for each state in which they do business. Acquiring money transmitter licenses for all 53 states is a costly and time consuming process. The estimated cost to become a licensed money transmitter in all 53 states amount to almost US$200,000 (surety bond fees, application fees, investigative fees etc.) and would take between one and three years.[155] These licensing requirements would greatly hamper the proliferation of these types of companies and limit entry into the market to those backed by large investors. As mentioned, these licenses are required for each state the company wishes to conduct business in. The New York Department of Financial Services (DFS) are actively developing a unique, virtual currency specific, called BitLicense. The DFS proposed the BitLicense regulatory framework in July 2014, which would require virtual currency businesses to be subject to specific capital requirements, financial examinations, recordkeeping and reporting requirements. The capital requirements include that the licensee must invest retained earnings and profits “only in high-quality, investment-grade permissible investments with maturities of up to one year and denominated in US dollars.”[156] The BitLicense framework aims to impose AML and KYC requirements for virtual currency related companies, in order to aid law enforcement and also to improve consumer protection, while still encouraging innovation. The proposal was open to public comment until October 2014, and was heavily criticized by the virtual currency community. Circle Internet Financial Inc., one of the largest virtual currency businesses, stated:

> Circle believes there are numerous areas in the Proposed Rule, which could negatively impact consumers and businesses that wish to utilize digital currencies. There are several requirements that are so burdensome (and in some cases nearly impossible to

[154] FinCEN. ‘Request for Administrative Ruling on the Application of FinCEN’s Regulations to a Virtual Currency Payment System’.2014. http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf

[155] ‘Money Transmitter Licensing’. *Grimes Law PPLC*,.2014, (accessed 30 October 2014), http://www.grimeslawaz.com/technology-and-licensing/money-transmitter-licensing/

To maintain the license would amount to approximately US$135,000 per annum.

[156] ‘New York Proposes BitLicense Regulations for Virtual Currency Businesses’, *Cleary Gottlieb*, 2014, (accessed 30 October 2014), http://www.cgsh.com/files/News/fb453ee8-2b46-404e-8922-c8e02d700c9e/Presentation/NewsAttachment/f3db9861-69e3-45bb-a7d4-ca408760ed24/New%20York%20Proposes%20BitLicense%20Regulations%20for%20Virtual%20Currency%20Businesses.pdf

> comply with) that if the Proposed Rule were to be enacted in its current form, Circle would have no choice but to exclude New York residents from its service.[157]

If the one of the largest virtual currency companies consider the requirements overly burdensome, there is little doubt that smaller companies would be able to comply. Voorhees states:

> "This will eliminate the college dorm room startup. It will eliminate the young entrepreneur who is willing to put in 100 hours per week, but who doesn't have $100,000 for his first two months of legal bills. It will make innovation the purview of large companies, which is to say, it will diminish innovation."[158]

Some Bitcoin related companies such as SatoshiBet, a large Bitcoin gambling website, have started excluding all U.S. citizens from accessing their services on account of the expected regulatory framework which is to be implemented in 2015.[159]

Regulators face a difficult task of mitigating the various risks associated with decentralized virtual currencies, and must find a way to protect consumers and prevent illegal activity that is not only cost-effective for regulators, but also allows the legitimate entities in the virtual currency economy to keep innovating and further developing these technologies.

7. Conclusion

Decentralized virtual currencies have rapidly become a reality and continues to evolve at an unprecedented rate. Bitcoin has emerged as potential new form of money which performs the functions of money in an innovative manner that does not rely on a central authority to facilitate transactions or confirm account balances. The absence of a central authority acting as an intermediary to transactions creates new opportunities, but also new potential risks. Users are able to independently, irreversibly and securely transfer value over the internet, with low transaction costs. With Bitcoin, the unbanked could become part of the global economy and the international migrant economy could be changed for the better. However, Bitcoin creates also complicated challenges for users and regulators, on due to its volatility and pseudonymous nature. On account of its pseudonymous nature, Bitcoin has been associated

---

[157] Tucker, M. 'Circle Submits Comments to NYDFS on Proposed BitLicense'. (accessed 30 October 2014). https://www.circle.com/en/2014/10/20/circle-submits-comments-nydfs-proposed-bitlicense

[158] 'Industry Reactions to New York's BitLicense Proposal', *CoinDesk* 2014, (accessed 30 October 2014), http://www.coindesk.com/new-york-bitlicense-views-inside-bitcoin-industry/

[159] 'SatoshiBet not planning to withdraw from more markets despite US exit', (accessed 31 October 2014), http://www.totallygaming.com/news/satoshibet-not-planning-withdraw-more-markets-despite-us-exit

with facilitating transactions for illicit goods and services, and could serve as a sophisticated tool for money laundering. Regulators have a difficult task of mitigating the risks associated with Bitcoin in a manner that does not drive technological innovation and the related economic development out of their borders.

Bitcoins primary innovation is the global public ledger, in which all transactions are recorded, and which is updated and secured by the entire network. This invention is still in early stages of its development: its evolution and future iterations cannot be accurately predicted. It is comparable how the internet was perceived in 1994. This analogy is formulated by Jimmy (2014) on Bit Blogger:

> Around 1994, the people that did anything on the internet at all were using it mostly for email. Some more savvy users maybe participated in newsgroups. A few very bleeding-edge people made web pages. You could have foreseen that there would be better versions of those things. What you couldn't foresee was stuff like VOIP [such as skype], Bittorrent [peer-to-peer downloads], video on demand or social networks. These are all technologies built on top of the internet and currently take up a large part of the traffic that goes through it.
>
> Email for most people in the 90′s was the first great killer app. It allowed people to communicate with each other without sending letters or making phone calls. Most people that knew about the internet in the early 90′s pointed to the post office as the first industry to get disrupted by the internet and to some degree they were right. What most people didn't see back then was that the internet would also disrupt the music store, the video rental store and to some degree, even the book store. In the same way, for most people bitcoin is a way to send money easily, so they point to Western Union and other money transmission businesses as the ones that will get disrupted. To a large degree they're right, but it's not the only one that'll get disrupted.[160]

Noteworthy applications that already exist include Counterparty (decentralized stock exchange based on block chain technology) , Ripple (decentralized money transfer), Storj.io (decentralized version of Dropbox), Proof of Existence (anonymously and securely store an online time-stamped distributed proof of existence for any document), BitPesa (remittance service for sending funds to Kenya), and OpenBazaar (open source, decentralized, cost free

[160] http://www.bitblogger.net/2014/07/10/the-great-unknown-bitcoin-killer-app/

marketplace). [161] Two exciting Swiss based projects that are yet to be launched include Ethereum and Monetas. Ethereum allows developers to build and publish their own distributed applications, potentially allowing decentralized secure forms of voting, domain name registries, financial exchanges, crowd-funding, company governance, smart contracts, intellectual property and even smart property through hardware integration. [162] Monetas, focused on financial inclusion, is developing a consumer mobile phone application to enable the unbanked masses to access to the global economy, as well as a "turnkey enterprise platform" that enables users to quickly and cheaply create businesses, complete with legal entity and payment system, all from a mobile phone.[163]

The invention of distributed ledger technologies will force various industries to become more competitive in the not-so-distant future. Tasks that up until the invention of Bitcoin required a trusted central authority can now be automated and become cheaper, quicker, more predictable and more secure than ever before. Block chain technology is here to stay, and while it is still relatively complicated and potentially risky to use, it is becoming more user friendly by the day. If mass consumer adoption becomes a reality, block chain applications could revolutionize the way we bank, transact and manage our assets.

[161] 'Startups around BlockChain technology`, 2014, (accessed on 30 October 2014), http://www.adesblog.com/startups-around-blockchain-technology/, http://counterparty.io/, https://ripple.com/, http://storj.io/, http://www.proofofexistence.com/, https://www.bitpesa.co/, https://openbazaar.org/.

[162] Ethereum, (accessed 25 October 2014), https://www.ethereum.org/

[163] Monetas Product Overview, (accessed 25 October 2014), http://monetas.net/products/

List of References

Ali, R. Barrdear, J. Clews, R. Southgate, J., ‘The economics of digital currencies’, *Bank of England Quarterly Bulletin2014 Q3*, 2014, (accessed 5 October 2014), http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf

Antonopoulos, A. M., *Mastering Bitcoin: Unlocking digital crypto-currencies*, O’Reily Media, 2014.

Bamford, C., *Principles of International Financial Law*, Oxford: Oxford University Press, 2011.

Bell, S., ‘The Hierarchy of Money’, *The Jerome Levy Economics Institute. Working paper No. 231*. 1998.

'Bitcoin - Turbulent Waters - Part Seven’, *Dorsey & Whitney LLP*, 2014. (Accessed 20 October 2014), http://www.dorsey.com/eu_cm_bitcoin_virtual_currency_pt7/

BitLegal. United States, 2014, (accessed 31 October 2014). http://bitlegal.io/nation/US.php

‘Blocks’, (accessed 25 October 2014), http://blockchain.info/blocks

Bryans, D., ‘Bitcoin and Money Laundering: Mining for an Effective Solution’, *Indiana Law Journal Vol. 89:441*, 2014.

Carney, M. ‘German’s Fidor bank will begin using Ripple for international wire transfers next week.’ *Pando Daily*.http://pando.com/2014/08/22/germans-fidor-bank-will-begin-using-ripple-for-international-wire-transfers-next-week/.

Chavez-Dreyfuss, G. ‘Exclusive: Overstock CEO says bitcoin sales to add 4 cents to 2014 EPS’. 2014. (Accessed 14 October 2014). http://www.reuters.com/article/2014/08/13/us-overstock-com-bitcoin-idUSKBN0GD21220140813

Cirasino, M. ‘How can we cut the high costs of remittances to Africa)’. 2013. (Accessed 20 October 2014), http://blogs.worldbank.org/psd/how-can-we-cut-the-high-costs-of-remittances-to-africa

Circle Financial Inc, 2014, (accessed on 25 October 2014), https://www.circle.com/en

Committee on Payment and Settlement Systems, ‘The role of central bank money in payment systems’, *Bank for International Settlements*, 2003.

CoinDesk. ‘Bitcoin ATM Map’. (accessed on 26 October 2014). http://www.coindesk.com/bitcoin-atm-map/

Conde, J. ‘Merchant Accounts 101’. 2013. (accessed 10 October 2014). http://www.merchant-account-services.org/article/merchant-accounts-101/11

Cook, R. J., ´Bitcoins: Technological innovation or Emerging Threat?´. *The John Marshall Journal of Information Technology and Privacy Law. Volume 30(3) 535*. 2014.

De Filipi, P., ‘Bitcoin: a regulatory nightmare to a libertarian dream’. *Internet Policy Review Vol. 3:2*. 2014. (accessed 20 October 2014), http://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream

‘Digital currencies: Quarterly Bulletin 2014 Q3 pre-release articles’. 2014. (accessed on 15 October 2014). http://www.bankofengland.co.uk/publications/Pages/quarterlybulletin/2014/qb14q3prereleasedigitalcurrenciesbitcoin.aspx

Dourado, E & Brito, J., 'Cryptocurrency, The New Palgrave Dictionary of Economics'. Eds. Steven N. Durlauf and Lawrence E. Blume, Palgrave Macmillan, 2014, (accessed 20 October 2014). http://www.dictionaryofeconomics.com/article?id=pde2014_C000625

Eatwell, J., Milgate, M., & Newman, P.*The new Palgrave dictionary of economics*, London:Macmillan, 2008.

Ethereum, (accessed 25 October 2014), https://www.ethereum.org/

European Central Bank, ‘Virtual Currency Schemes’. 2012. (accessed 10 October 2014), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European Central Bank, ‘EBA Opinion on ‘virtual currencies’, *EBA/Op/2014/08*, 2014.

‘Exchanges’,(accessed 25 October 2014)https://en.bitcoin.it/wiki/Exchanges

Fidor Bank. 2014. https://www.fidor.de/faq/ripple

FinCEN. ‘Request for Administrative Ruling on the Application of FinCEN’s Regulations to a Virtual Currency Payment System’.2014. http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf

FinCEN. ‘Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury’. *United States Financial Crimes Enforcement Network.* 2013.

Foley, S. ‘Bitcoin needs to learn from past e-currency failures’. *The Financial Times.* 2014. (accessed 25 October 2014). http://www.ft.com/cms/s/2/6d51117e-5806-11e3-a2ed-00144feabdc0.html

‘German Ministry of Finance declares Bitcoin payments sales-taxable’, *The Bundesverband Bitcoin, German affiliate of the Bitcoin Foundation* , 2014, (accessed 30 September 2014), http://www.bundesverband-bitcoin.de/?p=221

German Federal Financial Supervisory Authority, ‘BaFin Annual Report 2013’, 2014 , pp.58. (accessed 30 September 2014), http://www.bafin.de/SharedDocs/Downloads/EN/Jahresbericht/dl_annualreport_2013.pdf?__blob=publicationFile

Gilbert, R. N. & Blye A. D. ‘Bitcoin and Internet Payment Systems: Regulatory and Commercial Law Concerns’, *Carlton Fields Jorden Burt*, 2014, (accessed 30 September 2014), http://www.cfjblaw.com/bitcoin-internet-payment-systems-regulatory-and-commercial-law-concerns/#_edn15

Goodhart, C. A. E., ‘The two concepts of money: Implications for the analysis of optimal currency areas.’ *European journal of political economy, 14*(3). 1998.

‘Hackers hit web accounts of MtGox boss’, *BBC Technology News*, 2014. (Accessed 20 October 2014). http://www.bbc.com/news/technology-26387800

Hern, A., ‘US government prepares to auction $17m of seized Silk Road bitcoins’, *The Guardian.* 2014. (Accessed 24 Octber 2014), http://www.theguardian.com/technology/2014/jun/24/us-auction-seized-silk-road-bitcoins

How to Set Up a Merchant Account’. 2011. (Accessed 10 October 2014). http://paysimple.com/blog/2011/09/07/how-to-set-up-a-merchant-account/

‘How it Works, (accessed 25 October 2014),https://bitcoin.org/en/how-it-works

‘How Bitcoin Works, (accessed 25 October 2014), https://en.bitcoin.it/wiki/How_bitcoin_works

Inland Revenue Authority of Singapore. ‘GST treatment for e-Commerce transactions: Sale of virtual currency’, 2014, (accessed 30 September 2014), http://www.iras.gov.sg/irashome/page04.aspx?id=2276

‘Industry Reactions to New York’s BitLicense Proposal’, *CoinDesk* 2014, (accessed 30 October 2014), http://www.coindesk.com/new-york-bitlicense-views-inside-bitcoin-industry/

Ikeda, Y., ‘Carl Menger’s Monetary Theory: A Revisionist View’. *Keio University, Department of Economics,* 2008.

Jevons, W. S. ‘Money and the Mechanism of Exchange’. *Library of Economics and Liberty.* 1876. (accessed on 28 October 2014). http://www.econlib.org/library/YPDBooks/Jevons/jvnMME5.html

Jimmy, ‘The Great Unknown Bitcoin Killer App’, 2014, (accessed 30 October 2014), http://www.bitblogger.net/2014/07/10/the-great-unknown-bitcoin-killer-app/

Lamport, L., Shostak, R and Pease, M., 'The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems', July 1982, pages 382-401, as summarized by Jacobson, E. (accessed 6 October 2014), http://pages.cs.wisc.edu/~swift/classes/cs739-sp11/blog/2011/02/the_byzantine_generals_problem.html

Lo, S. Wang, J. C. 'Bitcoin as Money?'. *Current Policy Perspectives, Federal Reserve Bank of Boston No 14-4.* 2014.

Mankiw, N. G. & Taylor, P.M., *Economics. 2nd ed*. Andover : South-Western Cengage Learning, 2011.

Menger, C., 'On the Origins of Money'. *Economic Journal, Vol 2*, 1892, pp. 239-255.

Mersch, Y. 'Efficient retail payments - key in strengthening the competitiveness and growth potential of the EU'. 2014. (accessed on 25 October 2014). http://www.bis.org/review/r140324a.htm

Monetary Authority of Singapore, 'MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks', 2014. (accessed 30 September 2014), http://www.mas.gov.sg/news-and-publications/media-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.aspx

Monetas Product Overview, (accessed 25 October 2014), http://monetas.net/products/

'Money Transmitter Licensing'. *Grimes Law PPLC*,.2014, (accessed 30 October 2014), http://www.grimeslawaz.com/technology-and-licensing/money-transmitter-licensing/

Morphy, E., 'Bitcoin? Yawn. CheapAir Is Now Taking Litecoin and Dogecoin.', *Forbes*, 2014, (accessed 30 September 2014), http://www.forbes.com/sites/erikamorphy/2014/09/03/bitcoin-yawn-cheapair-is-now-taking-litecoin-and-dogecoin/

Nakamoto, S., 'Bitcoin: A Peer-to-Peer Electronic Cash system.', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

Nakamoto, S., Bitcoin Forum Post, 2009 (accessed 15 October 2014), https://bitcointalk.org/index.php?topic=99631.0

'New York Proposes BitLicense Regulations for Virtual Currency Businesses', *Cleary Gottlieb*, 2014, (accessed on 30 October 2014), http://www.cgsh.com/files/News/fb453ee8-2b46-404e-8922-c8e02d700c9e/Presentation/NewsAttachment/f3db9861-69e3-45bb-a7d4-ca408760ed24/New%20York%20Proposes%20BitLicense%20Regulations%20for%20Virtual%20Currency%20Businesses.pdf

Olafsonn, I. A., 'Is Bitcoin Money?: An analysis from the Austrian school of economic thought'. *Haskoli Islands University*, 2014.

Pacia, C., 'Bitcoin Mining Explained Like You're Five: Part 1 – Incentives', 2014, (accessed 10 October 2014) http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-1-incentives/
Payment Services Supervision Act of 25 June 2009 (Federal Law Gazette 1, p. 1506), as amended by Article 2 subsection (74) of the Act of 22 December 2011 (Federal Law Gazette I, p. 3044)

'Regulation of Bitcoin in Selected Jurisdictions'. *The Law Library of Congress*, *Global Legal Research Center.* 2014. (accessed on 10 October 2014). http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

'Regulation of Bitcoin in Selected Jurisdictions'. *The Law Library of Congress, Global Legal Research Center.* 2014. (accessed 10 October 2014). http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

Ron, D. Shamir, A., 'How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?', *Department of Computer Science and Applied Mathematics, The Weizmann Institute of Science, Israel*, 2013.

'Russia: Fines for Bitcoin Transactions Will Be Introduced'. (accessed 25 October 2014). http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205404151_text

'SatoshiBet not planning to withdraw from more markets despite US exit', (accessed 31 October 2014), http://www.totallygaming.com/news/satoshibet-not-planning-withdraw-more-markets-despite-us-exit

Semenova, A. ‘The Origin of Money: Enhancing the Chartalist Perspective’. *CFEPS*. 2007.
Shaheen, K. ‘Regulation of Bitcoin around the world´. *Lexology, Dentons.*2014. (accessed on 18 October 2014). http://www.lexology.com/library/detail.aspx?g=d92a33fe-3f11-43f6-b0cf-d8476ca612b1

Silk Road Bitcoin Auction Winner Tim Draper Won't Say How Many Millions He Paid. *Forbes.* 2014. (accessed 25 October 2014). http://www.forbes.com/sites/kashmirhill/2014/07/02/tim-draper-silk-road-bitcoin-auction/

Starr, R. M., ‘Why is there money? Endogenous derivation of "money" as the most liquid asset: A class of examples.’, *Economic Theory, 21(2/3)*, 2003.
Starr, R. M., ‘Money: in transactions and finance’. *Dept. of Economics, University of California, San Diego*. 1998.

‘State of Bitcoin Q3 2014’, CoinDesk, 2014, (accessed 20 October 2014). http://www.slideshare.net/CoinDesk/state-of-bitcoin-q3-2014?qid=a856ddfe-f3e9-4f61-8fa1-b60ba2340d19&v=qf1&b=&from_search=1

Trautman, L., ‘Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?’, *Richmond Journal of Law & Technology Volume XX(4)*, 2014, pp 86, (Accessed 28 October 2014). http://jolt.richmond.edu/v20i4/article13.pdf.

Tucker, M. ‘Circle Submits Comments to NYDFS on Proposed BitLicense’. (accessed 30 October 2014). https://www.circle.com/en/2014/10/20/circle-submits-comments-nydfs-proposed-bitlicense

‘Vocabulary’, (accessed 25 October 2014),https://bitcoin.org/en/vocabulary

‘Weaknesses’,(accessed 25 October 2014), https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

Wenzel, R. ‘Bitcoiners: Remember What Happened to eGold’. *Economic Policy Journal.* 2013. (accessed 24 October 2014). http://www.economicpolicyjournal.com/2013/04/bitcoiners-remember-what-happened-to.html

Wilber, D. Q., ‘Woman With Printer Shows the Digital Ease of Bogus Cash’, *Bloomberg*, 2014, (accessed 20 October 2014), http://www.bloomberg.com/news/2014-05-07/mom-with-hp-printer-shows-the-digital-ease-of-bogus-cash.html

‘What can you buy with Bitcoins?’,*Coindesk*, 2014, (accessed 29 September 2014), http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/
Wong, J. I., ‘Dark Markets Grow Bigger and Bolder in Year Since Silk Road Bust’, CoinDesk, 2014, (accessed 20 October 2014), http://www.coindesk.com/dark-markets-grow-bigger-bolder-year-since-silk-road-bust/

World Bank, ’Financial Inclusion’. Global Financial Development Report 2014. (acessed 14 October 2014). http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTGLOBALFINREPORT/0,,contentMDK:23489619~pagePK:64168182~piPK:64168060~theSitePK:8816097,00.html

Wright, G. ‘Is bitcoin good for business?’ *Global Finance, 28*(6). 2014. (accessed 10 October). http://bitcoinchamberofcommerce.com/?p=448

Bitcoin and Money Laundering: Mining for an Effective Solution

DANTON BRYANS*

INTRODUCTION

Technology forges ahead at a rapid pace, whether we like it or not. Criminals recognize this inevitability and use technological improvements to advance their craft,[1] committing crimes from half a world away in real time. Meticulous criminals also use technological advancements to distance themselves from their illegal activities and profits through use of virtual banking and electronic money transfer systems, which allow criminals to buy, sell, and exchange goods without any physical interaction. Though such services use digital logs that serve to identify a sender and a receiver's digital identities, criminals possess the means to obfuscate their digital identity by simply spoofing their Internet Protocol address or by using another individual's account, essentially making their activities untraceable.

New virtual currencies, such as Bitcoin, add yet another layer of anonymity by allowing users to transfer value without the collection of any personally identifiable information. Regulations often fail to affect such virtual currencies due to lack of foresight by the regulation writers, creating a legal gray area. Thus, criminals can continue to capitalize on technological innovation to bolster their illegal activities. Money laundering is one particular criminal craft that stands to benefit from technological advancement.

This Note analyzes the effects of Bitcoin and analogous virtual currencies on anti–money laundering (AML) enforcement. Part I gives a brief primer on money laundering and virtual currencies. Part II offers a Bitcoin primer, which differentiates Bitcoin technology from traditional currencies and competing virtual currencies. Part III analyzes whether Bitcoin is legal to use or trade in the United States, using domestic and international adoption of Bitcoin for guidance. Part IV discusses whether current U.S. AML regulatory schemes encompass the entirety of Bitcoin use, finding that it does not. Finally, Part V offers suggestions for a regulatory scheme encompassing Bitcoin and analogous virtual currency technologies. Ultimately, this Note recommends regulating Bitcoin currency exchanges under existing AML regulation schemes instead of broadening statutory definitions to control all aspects of Bitcoin or analogous virtual currencies.

---

* J.D. candidate 2014, Indiana University Maurer School of Law; B.S. 2011, Michigan State University. I began studying, mining, and trading on the Bitcoin network in early 2011. I am grateful to Professors Fred H. Cate, Sarah Jane Hughes, and Anthony J. Rose for their guidance; to my fellow *Indiana Law Journal* members for their help preparing for publication; and to my family for their support.

1. *See* Cyrus Farivar, *Man Accused of Placing GPS Device on Victim's Car Before Burglarizing Her Home*, ARS TECHNICA (Apr. 28, 2013, 11:22 AM), http://arstechnica.com/tech-policy/2013/04/man-accused-of-placing-gps-device-on-victims-car-before-burglarizing-her-home.

Attempting to regulate parties other than currency exchanges in the Bitcoin network will prove too onerous from a cost-benefit analysis perspective.[2]

I. MONEY LAUNDERING PRIMER

A. Money Laundering

Money laundering is "the process of making illegally-gained proceeds (i.e. 'dirty money') appear legal (i.e. 'clean')),"[3] and AML laws are the legislative attempts to curtail such illegal activity.[4] Criminals typically accomplish money laundering in three steps: (1) placement, where criminals inject dirty money into the financial system; (2) layering, where launderers transfer or convert dirty money to dissociate it from its illegal source; and (3) integration, where cleaned funds reenter the financial system in a seemingly legitimate state.[5] Due to the illegal character of the transactions, some organizations caution against attempting to estimate the total amount of money laundered per year;[6] however, the United Nations Office on Drugs and Crime (UNODC) report estimated the aggregate amount of laundered money to be approximately 2.7% of global GDP in 2009, or roughly $1.6 trillion.[7] In an increasingly digitized world, one question that emerges is whether innovative virtual currencies will make money laundering estimates and AML efforts more difficult for regulators and law enforcement.

B. Virtual Currencies

A virtual currency acts like a currency in some respects but is not directly akin to a real currency.[8] Virtual currency transactions are therefore different from simply

---

2. *See infra* Part V.

3. *History of Anti-Money Laundering Laws*, FIN. CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/news_room/aml_history.html [hereinafter *AML History*].

4. *See Anti-Money Laundering*, FIN. INDUS. REG. AUTHORITY, https://www.finra.org/Industry/Issues/AML.

5. *Money Laundering*, FIN. ACTION TASK FORCE, http://www.fatf-gafi.org/pages/faq/moneylaundering.

6. *Id.*

7. Yury Fedotov, *Preface* to UNITED NATIONS OFFICE ON DRUGS AND CRIME, ESTIMATING ILLICIT FINANCIAL FLOWS RESULTING FROM DRUG TRAFFICKING AND OTHER TRANSNATIONAL ORGANIZED CRIMES 5, 5 (2011), *available at* https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf; *see also* Michel Camdessus, Managing Dir., Int'l Monetary Fund, Address at the Plenary Meeting of the Financial Action Task Force on Money Laundering, Money Laundering: The Importance of International Countermeasures (Feb. 10, 1998), *available at* https://www.imf.org/external/np/speeches/1998/021098.htm (estimating in 1998 that the aggregate amount of money laundered was between 2% and 5% of global GDP, or roughly $590 billion and $1.5 trillion).

8. The Financial Crimes Enforcement Network (FinCEN) defines real currency as coin or paper money that circulates, is designated as legal tender, and is customarily used and accepted as a medium of exchange in the issuing country. Conversely, virtual currency "operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction."

transferring fiat currency[9] via an electronic medium (e.g., Automated Clearing House (ACH) transfers, PayPal).[10] Virtual currencies add another layer of complexity to AML efforts because, contrary to traditional currency transfer, there are no physical materials to observe or intercept for proof of illicit activities. Virtual currencies come in several formats: (1) physical, where a virtual currency is represented on a physical medium;[11] (2) centralized, where all transfers occur through an intermediary;[12] and (3) decentralized, where the network distributes transactions between nodes of a network, an example of which is Bitcoin.[13]

C. Bitcoin

Bitcoin is a decentralized, virtually anonymous[14] (commonly called pseudonymous),[15] peer-to-peer (transactions occur directly between users) network. Bitcoin's decentralization and peer-to-peer infrastructure allows it to be virtually immune to the risks of server raids or the loss of a central database to hackers.[16]

FIN. CRIMES ENFORCEMENT NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1 (2013) [hereinafter GUIDANCE], *available at* http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

9. A fiat currency is a "[c]ommon type of currency issued by official order, and whose value is based on the issuing authority's guarantee to pay the stated (face) amount on demand, and not on any intrinsic worth or extrinsic backing. All national currencies in circulation, issued and managed by the respective central banks, are fiat currencies." *Fiat Currency Definition*, BUSINESSDICTIONARY.COM, http://www.businessdictionary.com/definition/fiat-currency.html. It is also known as fiat money. *Fiat Money Definition*, INVESTOPEDIA, http://www.investopedia.com/terms/f/fiatmoney.asp. Examples are USD, EUR, etc. *See id.*

10. *Digital Currency*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Digital_currency (last modified Mar. 1, 2012).

11. One example of a physical virtual currency is the now defunct DigiCash. *See* Steven Levy, *E-Money (That's What I Want)*, WIRED, Dec. 1994, at 174.

12. An example of a centralized virtual currency is WebMoney. *See About*, WEBMONEY, http://www.wmtransfer.com/eng/about/.

13. BITCOIN PROJECT, http://bitcoin.org.

14. *Introduction*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Introduction (last modified July 14, 2013).

15. *See, e.g.*, Morgen E. Peck, *The Crytoanarchists' Answer to Cash*, IEEE SPECTRUM, June 2012, at 50, 56 ("Bitcoin is often described as providing pseudoanonymity, by creating enough obfuscation to provide users with plausible deniability."); Thomas Lowenthal, *Bitcoin: Inside the Encrypted, Peer-to-Peer Digital Currency*, ARS TECHNICA (June 8, 2011, 9:00 AM), http://arstechnica.com/tech-policy/2011/06/bitcoin-inside-the-encrypted-peer-to-peer-currency ("Bitcoin—a pseudonymous cryptographic currency . . ."). Pseudonymity is the use of a fictitious name or identity. BLACK'S LAW DICTIONARY 1347 (9th ed. 2009). In Bitcoin's case, this refers to the use of an alphanumeric string that represents the source or destination in a Bitcoin transfer. *Address*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Address (last modified Jan. 16, 2013). Thus, a pseudonym identifies the user instead of any personally identifiable information and is virtually anonymous to an onlooker to the transaction.

16. This does not mean Bitcoin currency exchanges cannot be hacked; it means that the Bitcoin protocol infrastructure is relatively safe. *See, e.g.*, Press Release, Mark Karpeles,

Due to the possibility of its use for nefarious activities such as money laundering, Bitcoin's pseudonymous network negatively impacted the image of emerging virtual currency systems, and some authorities view Bitcoin solely as a platform for criminals.[17] Whatever the perceived or potential economic role may be for Bitcoin,[18] the question remains as to how current U.S. Federal AML and state money transmitter laws will apply to Bitcoin and analogous technologies.

II. BITCOIN PRIMER

A. Comparison to Other Currency Systems

Bitcoin's inventor, Satoshi Nakamoto,[19] sought to create a system that would solve several issues with traditional fiat currency systems.[20] A traditional fiat currency system is vulnerable to inflation,[21] whereas Bitcoin for the most part, is not.[22] Cash and Bitcoin transactions are similarly anonymous or pseudonymous, but Bitcoin does not require face-to-face transactions. Finally, a governmental body backs a fiat currency, which provides reputational stability to the fiat currency that

---

Chief Exec. Officer, Tibanne Co. Ltd., Clarification of Mt. Gox Compromised Accounts and Major Bitcoin Sell-Off (June 30, 2011), https://mtgox.com/press_release_20110630.html.

17. *E.g.*, Mike Masnick, *Senator Schumer Says Bitcoin Is Money Laundering*, TECHDIRT (June 6, 2011, 9:26 AM), https://www.techdirt.com/articles/20110605/22322814558/senator-schumer-says-bitcoin-is-money-laundering.shtml; *see also* Letter from Charles E. Schumer & Joe Manchin, U.S. Senators, to Eric Holder, Att'y Gen. of the United States (June 6, 2011), *available at* http://manchin.senate.gov/public/index.cfm/press-releases?ID=284ae54a-acf1-4258-be1c-7acee1f7e8b3. Senators Schumer and Manchin urged the U.S. Attorney General and Drug Enforcement Agency to shut down Silk Road, an anonymous online marketplace used for selling illicit substances, which used Bitcoin as a currency. *Id.* The Senators referred to Bitcoin in the letter as "untraceable." *Id.*

18. Some view Bitcoin as a possible solution to the issues that fiat currencies face, such as government intervention and currency inflation. *See, e.g.*, Jon Matonis, *Bitcoin Prevents Monetary Tyranny*, FORBES (Oct. 4, 2012, 11:58 AM), http://www.forbes.com/sites/jonmatonis/2012/10/04/bitcoin-prevents-monetary-tyranny.

19. *See generally* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN PROJECT, http://bitcoin.org/bitcoin.pdf. Satoshi Nakamoto is most likely a pseudonym of the actual inventor or inventors of Bitcoin. *Satoshi Nakamoto*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Satoshi_Nakamoto (last modified June 13, 2013).

20. *See* Jon Matonis, *ECB: "Roots of Bitcoin Can Be Found in the Austrian School of Economics*,*"* FORBES (Nov. 3, 2012, 11:04 AM), http://www.forbes.com/sites/jonmatonis/2012/11/03/ecb-roots-of-bitcoin-can-be-found-in-the-austrian-school-of-economics (describing theoretical economical roots of Bitcoin).

21. *See, e.g.*, DavidC, *What Is the Significance of the Fiat Currency?*, INFLATIONDATA.COM (Sept. 20, 2012), http://inflationdata.com/articles/2012/09/20/significance-fiat-currency.

22. Colin Dean, Comment to *Why Are Fiat Currencies Inflationary and Bitcoin Deflationary?*, STACK EXCHANGE (Dec. 28, 2012, 5:30 PM), http://bitcoin.stackexchange.com/questions/5931/why-are-fiat-currencies-inflationary-and-bitcoin-deflationary ("Bitcoin's deflationary quality is based on the assertion that a currency must have scarcity in order to be valuable. By limiting what amount can enter the system, it ensures that no individual can increase the supply and inflate the value relative to physical goods.").

a new virtual currency inherently lacks. Trading in fiat currency will allow the parties to have relative faith in the currency's value as stated by the distributing government, but Bitcoin has no set value, and its value can fluctuate dramatically.[23] Thus, Bitcoin is less inflation prone and offers greater anonymity for the transacting parties, but it lacks the reputational security and trust associated with a fiat currency backed by the full faith and credit of a sovereign government.

Nakamoto also sought to solve several issues with centralized virtual currency systems with the Bitcoin system.[24] Virtual currency systems with centralized authority typically require users to have accounts so the central authority can administrate transactions;[25] a centralized system will also be vulnerable to attacks on the central infrastructure, possibly leading to a complete shutdown of the system.[26] However, the authority inherent in a central infrastructure gives assurance to users that issues with transactions and fraud on the network can be solved administratively.[27] Some users may wish to sacrifice anonymity and network security in exchange for such assurance against fraud, which the pseudonymous Bitcoin network cannot provide. Thus, compared to a centralized virtual currency system, the Bitcoin protocol is superior for anonymity and flexibility; however, Bitcoin lacks authoritative backing and central control.

B. Operational Overview

Bitcoin is a pseudonymous,[28] decentralized virtual currency system that operates purely by algorithm,[29] using bitcoin as the unit of currency.[30] No government sets a bitcoin's value; instead, supply and demand of Bitcoin users in the marketplace sets the value.[31] A Bitcoin user may obtain bitcoins by buying bitcoins from others[32] or

---

23. Bitcoin's value rose from $34 on March 6, 2013 to $266 by April 10, 2013, only to crash to approximately $104 (a 61% decline) in less than a day. Timothy B. Lee, *An Illustrated History of Bitcoin Crashes*, FORBES (Apr. 11, 2013, 12:45 AM), http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes.

24. *See* Lowenthal, *supra* note 15; Nakamoto, *supra* note 19.

25. *See Security Recommendations*, E-GOLD, http://www.e-gold.com/security.html; *Security*, PAYPAL, https://www.paypal.com/webapps/mpp/paypal-safety-and-security.

26. *See* Alison Gendar & John Marzulli, *Cops Bust Hackers Who Shut Down PayPal After Online Payment Service Cut Ties with WikiLeaks*, N.Y. DAILY NEWS (July 20, 2011, 4:00 AM), http://www.nydailynews.com/news/crime/cops-bust-hackers-shut-paypal-online-payment-service-cut-ties-wikileaks-article-1.159867.

27. *See* PAYPAL, *supra* note 25.

28. *See supra* note 15 and accompanying text.

29. *See, e.g.*, Lowenthal, *supra* note 15; Nicolás Mendoza, *Understanding Bitcoin*, AL JAZEERA, http://www.aljazeera.com/indepth/opinion/2012/05/20125309437931677.html (last modified June 9, 2012).

30. Note that the units of currency are lowercased (bitcoins), whereas the currency system and network are capitalized (Bitcoin). *Introduction*, *supra* note 14. Units of bitcoins are commonly represented as BTC. *Vocabulary*, BITCOIN PROJECT, http://bitcoin.org/en/vocabulary.

31. *See FAQ*, BITCOIN WIKI, https://en.bitcoin.it/wiki/FAQ (last modified July 24, 2013).

32. *Getting Started with Bitcoin*, WEUSECOINS, http://www.weusecoins.com/getting-started.php (discussing how to get bitcoins by completing bonus programs, trading with

by using their computer's processing power to help facilitate transactions on the Bitcoin network in a process called mining.[33]

Bitcoin transactions begin when a buyer transmits a quantity of bitcoins from his or her personal digital wallet[34] through a Bitcoin client[35] to the coded Bitcoin payment address representing the seller's digital wallet.[36] The Bitcoin network recognizes this broadcast of information, and each node (called a miner) of the network processes the transaction and adds the value of the transaction to the end of a coded string representing other recently broadcast transactions.[37] Miners then encode this "block" of recently broadcast transmissions onto the end of all the previous completed blocks[38] at a rate of approximately one block per ten minutes.[39] Finally, the individual miner who finalizes the block receives a set number of bitcoins.[40] To finalize a block and receive the bitcoin reward, the miner's calculated value of the block must match a generated value from the Bitcoin system, and the difficulty of matching this value modulates as the total computational power from the miners in the network increases to maintain the ten-minute completion rate.[41] Once a block finalizes, that transaction is practically irreversible without controlling the majority of the network's processing power.[42] Thus, there will be a relatively predictable payout of bitcoins following the predetermined block creation rate until the total number of BTC reaches a preset cap of 21 million bitcoins, and

---

local Bitcoin users, purchasing through currency exchanges, and trading directly with other Bitcoin users online).

33. *See* Peck, *supra* note 15, at 56.

34. A Bitcoin wallet is a digital container where a Bitcoin user can store data referring to the user's addresses, transactions, preferences, etc. *Wallet*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Wallet (last modified Mar. 31, 2013). A user may choose from several forms of digital wallets. Vitalik Buterin, *Bitcoin Wallet Reviews–Ease of Use and Security*, BITCOIN MAG. (Mar. 5, 2012), http://bitcoinmagazine.com/bitcoin-wallet-options.

35. Clients can create and interface with Bitcoin wallets, allowing the user to send and receive bitcoins. *See* WEUSECOINS, *supra* note 32.

36. *See* Peck, *supra* note 15, at 54.

37. *Id.* at 54–55. A miner is a user that uses his or her computer's resources to try to process and verify transactions on the Bitcoin network into blocks by way of mathematical calculations. *See Vocabulary*, *supra* note 30.

38. This is called a block chain. Peck, *supra* note 15, at 55–56; *see also Block Chain*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Block_chain (last modified May 18, 2013) (providing more background and technical data of block chain design).

39. *FAQ*, *supra* note 31.

40. Peck, *supra* note 15, at 56. This block completion reward halves once half of all remaining bitcoins have been produced, which will occur approximately once every four years. The reward halved from 50 BTC to 25 BTC on November 28, 2012. *See* Adrianne Jeffries, *Total Number of Bitcoins Hits 10.5 Million, Production Halves to Stop Inflation*, VERGE (Nov. 28, 2012, 10:44 AM), http://www.theverge.com/2012/11/28/3701434/total-number-of-bitcoins-hits-10-5-million-production-halves-to-stop. This system is intended to simulate the scarcity of a limited resource commodity, such as gold, and prevent inflation. Vitalik Buterin, *Block Reward Halving: A Guide*, BITCOIN MAG. (Nov. 27, 2012), http://bitcoinmagazine.com/block-reward-halving-a-guide.

41. *See* Buterin, *supra* note 40.

42. *See id.* ("[A]fter four to six blocks, any attempt to fraudulently change the transaction history to your own benefit becomes impractical because of all the work that has already been done overtop.").

the strength of the network itself would theoretically prevent fraudulent reversed transactions.

A typical Bitcoin transaction, including those that involve money laundering activities, includes approximately five entities: (1) a Bitcoin sender that initiates the transaction on the network, in this case with dirty money; (2) a Bitcoin receiver who accepts the bitcoins, or in this case the launderer who helps the sender obfuscate the dirty money's source; (3) Bitcoin miners that act as transaction verifiers and processors by completing blocks, sometimes for a nominal fee; (4) the core Bitcoin development team, which updates the Bitcoin codebase as necessary; and (5) Bitcoin currency exchanges, which facilitate conversion of bitcoins to other currencies and vice versa. This Note principally examines possible legal actions in light of these five entities.

C. Differences Affecting Money Laundering

The primary features of Bitcoin that prove beneficial to its survival, and harmful to effective AML regulation, are the protocol's anonymity and resilience through flexibility. Without being able to tie an identifiable user to a single Bitcoin address, tracking the injection, layering, and reentry of laundered funds would be extremely difficult for enforcement entities. Additionally, as each mining node of the Bitcoin network receives and processes all transactions, and the Bitcoin network automatically scales the difficulty for completing blocks based on the total processing power of all miners, stopping the Bitcoin network from functioning requires disabling every miner on the network.[43] Therefore, AML efforts face a target that is both difficult to identify and essentially impervious to interruption.

Bitcoin potentially allows any user—legitimate or criminal—to transfer money at near instantaneous speed at little or no cost, with very low barriers to entry, while remaining virtually anonymous without what could otherwise require a public paper trail. Users' abilities to exchange bitcoins directly for other currencies, to transfer through an endless number of different Bitcoin addresses for obfuscation, and to trade with other users for physical goods further frustrates AML efforts. Essentially, Bitcoin and analogous virtual currencies could enable money launderers to move illicit funds faster, cheaper, and more discretely than ever before.

III. LEGALITY OF BITCOIN IN THE UNITED STATES

A. Constitutional Limits on Currency

Although Bitcoin may frustrate AML efforts, discussion of solutions under current AML frameworks is unnecessary if Bitcoin is unconstitutional per se. Bitcoin might be seen as illegal because it attempts to assume powers expressly reserved to the federal government under the U.S. Constitution; however, Bitcoin

---

43. *See supra* note 41 and accompanying text. Even if only a single miner remained, the network will allow a block to be created approximately every ten minutes, and transactions will still process on the network.

likely falls outside of these powers. The U.S. Constitution reserves rights for the federal government to coin money for the nation,[44] to regulate value of the nation's coin,[45] to prosecute counterfeiters,[46] and it prohibits states from coining money.[47] However, the federal government appears to allow local currencies when there appears to be no likelihood of confusion with the nation's currency.[48] Conversely, the federal government has prosecuted currencies that pass off as the nation's legitimate currency.[49] Thus, as a purely digital currency, the likelihood that Bitcoin would be confused with the nation's federal currency is quite low.[50] Although Congress could potentially restrict Bitcoin or other virtual currencies through legislative action, perhaps through its Commerce Clause powers,[51] the clauses that relate to the coining of money should not render Bitcoin inherently illegal.

B. Bitcoin's Image in the United States

Bitcoin's image within the United States is polarized. Some view it as a tool used by criminals to commit crimes,[52] whereas others view it as a tool for a legal system of currency that is free from unlawful government interference.[53] Most notably, in 2011 Senators Charles Schumer and Joe Manchin denounced Bitcoin in a letter to U.S. Attorney General Eric Holder and the Drug Enforcement Administration (DEA) as "[t]he only method of payment" for an illegal Internet

---

44. U.S. CONST. art. I, § 8, cl. 5 ("To coin Money").

45. *Id.* ("To . . . regulate the Value thereof, and of foreign Coin").

46. *Id.* art. I, § 8, cl. 6 ("To provide for the Punishment of counterfeiting the Securities and current Coin of the United States").

47. *Id.* art. I, § 10, cl. 1 ("No State shall . . . coin Money . . . [or] make any Thing but gold and silver Coin a Tender in Payment of Debts . . . .").

48. *See* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 182 (2012) ("However, organizations have been issuing a certain type of private currency—community currencies meant to circulate only within a particular community—in the U.S. for decades. Government officials have known about these currencies and have commented that they seem to pose no threat."). One such example is the Ithaca Hours local alternative currency. ITHACA HOURS, http://www.ithacahours.com.

49. *See* Grinberg, *supra* note 48, at 191–94; Alan Feuer, *Prison May Be the Next Stop on a Gold Currency Journey*, N.Y. TIMES, Oct. 25, 2012, at A18; *see also Private Tender: Anti-Government Group Mints Its Own Coins*, FED. BUREAU INVESTIGATION (Apr. 5, 2011), http://www.fbi.gov/news/stories/2011/april/dollar_040511/dollar_040511.

50. The federal government unsuccessfully attacked several private payment articles using the Stamp Payments Act of 1862 when the articles were too dissimilar from official U.S. currency or contrary to the purposes of the Act. *See* Grinberg, *supra* note 48, at 183–85. Because virtual currencies bear little resemblance to official U.S. currency, and the applicability of a statute over 150 years removed from modern society is questionable, it is unlikely that the government could entirely limit virtual currencies through the Stamp Payments Act. *See id.* at 186–91.

51. It seems likely that the sale or use of bitcoins to buy goods or fiat currency would have interstate effects.

52. *See supra* note 17 and accompanying text.

53. *See, e.g.*, evoorhees, Comment to *How Do You Feel About Market Regulation?*, BITCOIN F. (July 4, 2011, 3:41 AM), https://bitcointalk.org/index.php?topic=25653.msg321165#msg321165.

marketplace called Silk Road.[54] More recently, an anonymous group claimed to steal copies of presidential candidate and former Massachusetts Governor Mitt Romney's tax records and threatened to release them to the public if the group did not receive $1 million worth of bitcoins.[55]

In addition to the specific uses of Bitcoin for illegal activities, some agencies examined Bitcoin for more general law enforcement concerns. A leaked U.S. Federal Bureau of Investigation (FBI) report from April 2012 examined the challenges created by Bitcoin for law enforcement.[56] The report's summary notes that the FBI (1) has "medium confidence that, in the near term, cyber criminals will treat Bitcoin as another payment option alongside more traditional and established virtual currencies which they have little reason to abandon"[57] and (2) has "low confidence, based on current user and vendor acceptance, that malicious actors will exploit Bitcoin to launder money."[58] Although the report mentions several possible illegal uses for Bitcoin, including laundering money and trading illicit goods, the report never categorizes Bitcoin as inherently illegal. Although the FBI does not explain this lapse in the report, the most likely reason is that it may be used for other legitimate purposes. Just as a hundred dollar bill may buy a family's groceries or an addict's drugs, so too could a bitcoin buy both legal and illegal goods.

Although some may use Bitcoin for illegal purposes, others see it as a viable alternative for private individuals to trade value. In essence, Bitcoin proponents see the virtual currency as either (1) an alternative currency or (2) a commodity.[59] In the first view, the bitcoins are functionally equivalent to USD, EUR, or any other currency system.[60] Alternatively, bitcoins act as commodities, similar to purchased goods.[61] Under either theory, the use of bitcoins should be lawful.[62]

---

54. *See supra* note 17 and accompanying text.

55. Josh Levs, *Group Claiming to Have Romney Tax Records Threatens to Leak Them*, CNN.COM (Sept. 6, 2012, 4:45 PM), http://www.cnn.com/2012/09/06/politics/romney-tax-threat/index.html; *see also* Jay Hathaway, *Blackmailers Make $50 on Romney's Tax Returns*, DAILY DOT (Sept. 28, 2012), http://www.dailydot.com/news/blackmailers-50-dollars-bitcoin-romney-taxes (stating the ransom was not paid and the blackmailers only made about $50).

56. FBI DIRECTORATE OF INTELLIGENCE, CYBER INTELLIGENCE SECTION & CRIMINAL INTELLIGENCE SECTION, BITCOIN VIRTUAL CURRENCY: UNIQUE FEATURES PRESENT DISTINCT CHALLENGES FOR DETERRING ILLICIT ACTIVITY (2012) [hereinafter FBI REPORT], *available at* http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf.

57. *Id.* at 2 (footnote omitted).

58. *Id.*

59. *See, e.g.*, evoorhees, Comment to *Let's End One Debate: Commodity vs Money*, BITCOIN F. (Oct. 7, 2011, 1:13 AM), https://bitcointalk.org/index.php?topic=47111.msg560958#msg560958; NewLibertyStandard, Comment to *Definition of a Commodity & Are Bitcoins a Commodity?*, BITCOIN F. (Aug. 14, 2010, 8:40 PM), https://bitcointalk.org/index.php?topic=815.msg9258#msg9258.

60. *See* Richard Satran, *How Did Bitcoin Become a Real Currency?*, U.S. NEWS & WORLD REP. (May 15, 2013), http://money.usnews.com/money/personal-finance/articles/2013/05/15/how-did-bitcoin-become-a-real-currency.

61. *See* Steve Forbes, *Bitcoin: Whatever It Is, It's Not Money!*, FORBES (Apr. 16, 2013, 10:50 AM), http://www.forbes.com/sites/steveforbes/2013/04/16/bitcoin-whatever-it-is-its-not-money.

62. Bitcoin users probably will also need to lawfully disclose any earnings for tax purposes. The IRS has not issued guidance specifically on this issue, although some believe

Bitcoin also gained some governmental acceptance at the state level. In July 2012, New Hampshire State Representative Mark Warden began accepting donations to his campaign through Bitcoin.[63] Shortly thereafter, Vermont State Senate candidate Jeremy Hanson verified Bitcoin's use for donations to be acceptable with two Vermont offices before also accepting contributions through Bitcoin.[64] Thus, it appears some politicians are willing to accept the system, at least when it comes to receiving contributions, and some state governments allow Bitcoin's use as well.

Finally, on March 18, 2013, the Financial Crimes Enforcement Network ("FinCEN") issued interpretive guidance for applying FinCEN's regulations to virtual currencies.[65] FinCEN primarily administers compliance with the Bank Secrecy Act (BSA), discussed in detail in Part IV of this Note.[66] Though not identifying Bitcoin by name, FinCEN clearly meant to include Bitcoin under its "De-Centralized Virtual Currencies" section of the guidance.[67] Some have viewed this as validating Bitcoin's legitimacy in the United States,[68] but others disagree.[69] Patrick Murck of the Bitcoin Foundation noted that FinCEN does not have authority to promulgate new rules without first going through the required notice and comment proceeding of the Administrative Procedures Act.[70] Realistically, although FinCEN's acknowledgment of Bitcoin is promising, the guidance does little to clarify Bitcoin's legal status beyond the BSA.

---

it will. *See* Robert W. Wood, *IRS Takes a Bite Out of Bitcoin*, FORBES (May 2, 2013, 3:40 AM), http://www.forbes.com/sites/robertwood/2013/05/02/irs-takes-a-bite-out-of-bitcoin. However, taxation of Bitcoin or other virtual currencies is beyond the scope of this Note.

63. BitPay, *Accepting Bitcoin for Political Campaign Donations*, HOW TO ACCEPT BITCOIN (Sept. 1, 2012, 5:03 PM), http://www.howtoacceptbitcoin.com/2012/09/accepting-bitcoin-for-political.html.

64. Jahvt, *Vermont State Senate Candidate Accepts Bitcoin Contributions*, VT. ELECTION WORKING GROUP (Sept. 24, 2012), http://vermontelection.org/2012/09/24/bitcoin (candidate verified Bitcoin's appropriateness as campaign contribution with both the Vermont Secretary of State's office and the Vermont Attorney General's office, finding "that Bitcoin-denominated contributions can be legally accepted and documented as 'in-kind' donations, so long as the donations [meet campaign contribution requirements]").

65. GUIDANCE, *supra* note 8.

66. *See infra* Part IV.A.1.

67. GUIDANCE, *supra* note 8, at 5 ("[A] de-centralized convertible virtual currency [is one] (1) that has no central repository and no single administrator, and (2) that persons may obtain by their own computing or manufacturing effort.").

68. *E.g.*, Michael Carney, *Bitcoin Is Legal, but Mainstream Adoption Will Mandate Playing by the Rules*, PANDODAILY (May 17, 2013), http://pandodaily.com/2013/05/17/bitcoin-is-legal-but-mainstream-adoption-will-mandate-playing-by-the-rules.

69. *E.g.*, WiW, Comment to *Bitcoins Are Not "Legalized" in the US–Understanding FinCEN's Announcement*, BITCOIN F. (Mar. 19, 2013, 2:51 PM), https://bitcointalk.org/index.php?topic=154905.msg1642139#msg1642139.

70. Patrick Murck, *Today, We Are All Money Transmitters . . . (No, Really!)*, BITCOIN FOUND. BLOG (Mar. 19, 2013), https://bitcoinfoundation.org/blog/?p=152.

C. Bitcoin's Image in the International Community

The international community appears largely in favor of allowing Bitcoin's legitimate use. A spokesperson for the Bank of Finland recently stated that people can use whatever currency they wish and that Bitcoin is legal to use in Finland.[71] A 2012 report by the European Central Bank examined Bitcoin as a virtual currency.[72] The report concluded that, under the European Union legal framework, Bitcoin most likely does not fall under the Electronic Money Directive,[73] stating, "Bitcoin clearly falls outside the scope of the Payment Services Directive."[74] The report additionally noted that, although such virtual currency schemes did not pose risk to the price stability of traditional currencies and do not fall within current regulation schemes, they did fall within the central bank's responsibility.[75] This means, at least for now, that Bitcoin shares characteristics with established payment systems in the European Union but is currently not under regulation schemes.

The German Federal Financial Supervisory Authority, BaFin, determined that Bitcoin is not "E-Geld"—roughly e-money or digital money—even though bitcoins serve the same economic function as E-Geld.[76] BaFin also found that currencies like Bitcoin hold monetary value as units of account and therefore fall under the definition of a financial instrument of payment.[77] This implies that Bitcoin service providers will fall within the definition of a financial services business and would require a license from BaFin to legally operate in Germany.[78] Thus, Bitcoin itself is

---

71. TehMatoking, *Ajankohtainen Kakkonen: Bitcoin [English Subtitles]*, YOUTUBE (Sept. 12, 2012), http://www.youtube.com/watch?v=7vYH1JH73pw (spokesperson for Bank of Finland replies to a question on a news report for Finnish TV about whether Bitcoin was illegal in Finland, roughly stating that people are free to invest in and use whatever forms of money that they prefer, at 3:30–4:20); *see also BitPay Exceeds 1,000 Merchants Accepting Bitcoin*, BITPAY (Sept. 11, 2012, 8:52 AM), http://blog.bitpay.com/2012/09/bitpay-exceeds-1000-merchants-accepting.html.

72. EUROPEAN CENT. BANK, VIRTUAL CURRENCY SCHEMES (2012) [hereinafter EU REPORT], http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. This means that Bitcoin is not regulated by a key European Union regulation initiative that "creat[ed] single, cross-border deposit accounts and harmoniz[ed] payment obligations and laws for credit transfers, direct debits, and payment cards across borders and payment instruments." Amelia H. Boss, *Convergence in Electronic Banking: Technological Convergence, Systems Convergence, Legal Convergence*, 2 DREXEL L. REV. 63, 64 (2009).

73. Council Directive 2009/110, 2009 O.J. (L 267) 7 (EC).

74. EU REPORT, *supra* note 72, at 43.

75. *Id.* at 47.

76. *Merkblatt—Hinweise zu dem Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz—ZAG)* [Data Sheet—Notes to the Act on the Supervision of Payment Services (Payment Services Oversight Act—ZAG)], BUNDESANSTALT FÜR FINANZDIENSTLEISTUNGSAUFSICHT (Dec. 22, 2011) (Ger.), http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html [hereinafter BAFIN]. The definition of E-Geld in section (4)(b) roughly states that bitcoins fall outside the definition of e-money, even though they are functionally the same as e-money, and are more similar to units of value like barter or private payment systems.

77. *See id.*

78. Akka, Comment to *An English Analysis on BAFIN?*, BITCOIN F. (Oct. 20, 2012,

legal under German law; however, businesses that would transact and hold customer funds from Bitcoin would need to have a license and would be regulated as such an entity.

A 2012 Australian Transaction Reports and Analysis Centre (AUSTRAC) report examined digital currencies, including Bitcoin, for use in criminal activities[79] and specifically looked at their use in money laundering.[80] The report concluded that digital currencies generally fall outside AML legislation globally and that digital currency exchanges could provide criminals with the ability to serially convert their digital currencies to other digital currencies before reintroduction as a fiat currency.[81] However, the report notes that use of digital currencies for illegal activities is not without drawbacks, citing the limited size of the digital currency markets and the limited rate of acceptance for payment.[82] It concluded, overall, that digital currencies "may currently be limited to niche crimes in the cyber environment and individual or smaller scale illicit activity."[83] This tone resonates with the seemingly apathetic opinion of the FBI report on Bitcoin.[84]

D. Widespread Use

Despite the possibility of using Bitcoin for illegal activity, only a few U.S. cases have dealt with Bitcoin's use, and none of those cases has specifically dealt with the question of Bitcoin's legality. The first Bitcoin case in the United States, between TradeHill, a Bitcoin exchange, and Dwolla, a payment processor, involved multiple causes of action.[85] However, the court vacated the lawsuit, compelling the parties to arbitrate.[86]

In a later case, users of a Bitcoin exchange filed suit against Bitcoinica, a Bitcoin exchange.[87] After a class action suit failed to attract sufficient support,[88]

12:48 PM), https://bitcointalk.org/index.php?topic=119425.msg1285574#msg1285574.

79. AUSTRALIAN TRANSACTION REPORTS & ANALYSIS CTR., TYPOLOGIES AND CASE STUDIES REPORT 2012, at 16–19 (2012) [hereinafter AUSTRAC REPORT], http://www.austrac.gov.au/files/typ_rprt12_full.pdf.

80. *Id.* at 19.

81. *Id.*

82. *Id.* at 17.

83. *Id.*

84. *See supra* text accompanying notes 56–58.

85. Complaint for Damages Resulting from: 1) Violation of 18 U.S.C. § 1964(c); 2) False Advertising; 3) Breach of Contract; 4) Intentional Misrepresentation; 5) Negligent Misrepresentation; 6) Concealment; 7) Restitution After Rescission; 8) Conversion; & 9) Defamation, TradeHill, Inc. v. Dwolla, Inc., No. CV 12 1082 JSC (C.D. Cal. Mar. 5, 2012), 2012 WL 1601094.

86. Order Granting Defendant's Motion to Compel Arbitration; Denying as Moot Defendants' Alternative Motion to Dismiss; Vacating Hearing, TradeHill, Inc. v. Dwolla, Inc., No. C-12-1082 MMC (N.D. Cal. May 9, 2012), 2012 WL 1622668.

87. Complaint for: (1) Breach of Contract; (2) Open Book Account; (3) Account Stated; (4) Negligence; & (5) Conversion, Cartmell v. Bitcoinica LP, No. CGC-12-522983 (Cal. Super. Ct. Aug. 6, 2012) [hereinafter Bitcoinica Complaint].

88. *See Class Action Litigation vs. Bitcoinica Consultancy LTD & Intersango LTD*, BITCOIN F. (July 13, 2012, 3:11 PM), https://bitcointalk.org/index.php?topic=93109.0;all (former Bitcoinica users discussing legal action with no eventual consensus).

four users filed suit individually.[89] The users alleged multiple losses of user funds due to hacks against the website.[90] The court denied the defendant's motion to dismiss the trial[91] and continued accepting motions.

Finally, the SEC brought an action against Trendon Shavers, owner of the former Bitcoin Savings & Trust,[92] for violations of the Securities Act of 1933 and the Exchange Act of 1934.[93] Magistrate Judge Mazzant of the U.S. District Court of the Eastern District of Texas stated, in response to Shaver's challenge of the court's subject matter jurisdiction over the case,[94] "[i]t is clear that Bitcoin can be used as money."[95] The court further determined that "the [Bitcoin Savings & Trust] investments meet the definition of investment contract, and as such, are securities" and found that the court had subject matter jurisdiction to preside over the case.[96]

Besides these cases, a few other notable events made headlines, including the unexpected shutdowns of Bitfloor[97] and TradeHill,[98] major Bitcoin exchanges, and an online digital wallet provider, MyBitcoin.[99] However, the owners of these services initiated the shutdowns, not the government.[100] The low number of lawsuits may be due in part to an aversion to governmental authority on the part of Bitcoin users,[101] but the fact remains that no court has specifically examined Bitcoin's legality.

Another indicator of whether Bitcoin is considered legal is its adoption by businesses and organizations and the lack of government intervention against these

---

89. Bitcoinica Complaint, *supra* note 87, at 1.

90. Adrianne Jeffries, *Bitcoin Woes: Users File Lawsuit over $460k in Missing Funds*, VERGE (Aug. 10, 2012, 4:20 PM), http://www.theverge.com/2012/8/10/3233711/second-bitcoin-lawsuit-is-filed-in-california.

91. Cartmell v. Bitcoinica, No. CGC-12-522983 (Cal. Super. Ct. Jan. 28, 2013) (order denying motion to dismiss or stay action).

92. *See* Todd Mokos, *SEC Files Charges Against Bitcoin Ponzi Mastermind Trendon Shavers*, BITCOIN MAG. (July 24, 2013), http://bitcoinmagazine.com/5889/sec-files-charges-against-bitcoin-ponzi-mastermind-trendon-shavers/. Some believe that the Bitcoin Savings & Trust was a Ponzi scheme. *Id.*; *see also* Adrianne Jeffries, *The Bernie Madoffs of Bitcoin? As Market Heats Back Up, Virtual Hedge Funds Claim Fantastical Profits*, VERGE (Aug. 15, 2012, 2:27 PM), http://www.theverge.com/2012/8/15/3243200/bitcoin-ponzi-schemes-savings-and-trust.

93. Complaint, SEC v. Shavers, No. 4:13CV-00416 (E.D. Tex. July 7, 2013).

94. SEC v. Shavers, No. 4:13-CV-416, at 1 (E.D. Tex. Aug. 6, 2013) (opinion regarding the court's subject matter jurisdiction).

95. *Id.* at 3.

96. *Id.* at 4.

97. Cyrus Farivar, *Bitfloor, Number Four Bitcoin-Based Exchange, Shuts Down for Good*, ARS TECHNICA (Apr. 18, 2013, 10:36 AM), http://arstechnica.com/business/2013/04/bitfloor-number-four-bitcoin-based-exchange-shuts-down-for-good.

98. Timothy B. Lee, *Major Bitcoin Exchange Shuts Down, Blaming Regulation and Loss of Funds*, ARS TECHNICA (Feb. 15, 2012, 10:15 AM), http://arstechnica.com/tech-policy/2012/02/major-bitcoin-exchange-shuts-down-blaming-regulation-and-loss-of-funds.

99. Adrianne Jeffries, *Search for Owners of MyBitcoin Loses Steam*, BETABEAT (Aug. 19, 2011, 10:15 AM), http://betabeat.com/2011/08/search-for-owners-of-mybitcoin-loses-steam.

100. *See* Farivar, *supra* note 97; Jeffries, *supra* note 99; Lee, *supra* note 98.

101. Jeffries, s*upra* note 90.

businesses and organizations. Many individuals and online businesses have voiced support for—or have begun to accept payments through—Bitcoin,[102] including security-consulting firms, Internet-hosting companies, food services, and nonprofit companies.[103] Some businesses also facilitate the conversion of bitcoins to fiat currencies.[104] Again, none of these organizations have been shut down due to use of Bitcoin itself.[105] As the U.S. government previously stopped currencies[106] and virtual currencies[107] that the government found to violate U.S. currency laws, and stopped companies that operate under state laws in conflict with federal law,[108] the lack of any such action by the U.S. government indicates that it either tolerates Bitcoin as an unregulated virtual currency or believes that current laws adequately regulate Bitcoin.

However, some organizations either have stopped accepting Bitcoin donations or have refused to accept them outright. The Electronic Frontier Foundation, a notable advocate for digital privacy rights, initially accepted Bitcoin donations, then stopped due to legal uncertainties in 2011,[109] and then resumed accepting donations in 2013 after the FinCEN guidance.[110] Additionally, Wikimedia, the nonprofit organization that runs Wikipedia, rejected the use of Bitcoin for donations, stating that "[Wikimedia] do[es] not accept 'artificial' currencies—that is, those not backed by the full faith and credit of an issuing government."[111]

---

102. *See, e.g.*, Andy Skelton, *Pay Another Way: Bitcoin*, JUST ANOTHER WORDPRESS WEBLOG (Nov. 15, 2012, 10:21 PM), http://en.blog.wordpress.com/2012/11/15/pay-another-way-bitcoin (announcing official WordPress acceptance of Bitcoin transactions).

103. *See Trade*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Trade (last modified Oct. 22, 2013) (listing services and organizations that accept Bitcoin payments).

104. *See, e.g.*, BITPAY, https://bitpay.com; PAYSIUS, http://paysius.com.

105. Most shutdowns of legitimate businesses seem to be due to lack of or loss of funds. *See, e.g.*, Lee, *supra* note 98. Many of the illegal shutdowns are due to other violations. *See supra* notes 85–101 and accompanying text.

106. Grinberg, *supra* note 48, at 191–94 (discussing the Liberty Dollar currency).

107. *Id.* at 204–06 (discussing the e-gold currency).

108. *Cf.* Meredith Bennett-Smith, *DEA Raids Legal Medical Marijuana Dispensaries in Washington, 'Humiliating' Shop Owners*, HUFFINGTON POST (July 25, 2013, 2:55 PM), http://www.huffingtonpost.com/2013/07/25/dea-raid-marijuana-dispensaries-washington-state_n_3653071.html. The federal government has made no statement to date explicitly rejecting Vermont's position on accepting Bitcoin for campaign donations.

109. Cindy Cohn, *EFF and Bitcoin*, ELECTRONIC FRONTIER FOUND. (June 20, 2011), https://www.eff.org/deeplinks/2011/06/eff-and-bitcoin.

110. Cindy Cohn, Peter Eckersley, Rainey Reitman & Seth Schoen, *EFF Will Accept Bitcoins to Support Digital Liberty*, ELECTRONIC FRONTIER FOUND. (May 17, 2013), https://www.eff.org/deeplinks/2013/05/eff-will-accept-bitcoins-support-digital-liberty. However, the EFF does not accept bitcoins directly, instead using BitPay to convert the bitcoins. *Id.*

111. Maggie Dennis, *Answers Archive/November 2011*, WIKIMEDIA FOUND. (Nov. 3, 2011, 8:33 PM), https://wikimediafoundation.org/wiki/Answers_archive/November_2011#Finance:_Why_does_the_Wikimedia_Foundation_not_currently_accept_Bitcoin.3F. Interestingly, BitPay, a Bitcoin payment processor that converts bitcoins to fiat currencies, announced that it would allow Bitcoin users to donate their bitcoins to Wikipedia by processing the transactions to USD and then donating the result to Wikipedia at no charge. *Donate to Wikipedia with Bitcoin*, BITPAY (Nov. 29, 2012, 11:13 AM), http://blog.bitpay.com/2012/11/donate-to-wikipedia-with-bitcoin.html.

Overall, this displays some hesitation to accept Bitcoin by some; however, it hardly shows rejection of Bitcoin at large.

E. Bitcoin Is Legal

The domestic and international outlooks on the legality of virtual currencies are somewhat complimentary, and a more comprehensive picture emerges when viewing the two outlooks simultaneously. Both domestic and international parties share the view that Bitcoin is not inherently illegal; however, international views tend to specify that Bitcoin is a legal currency. As Bitcoin's founder computed the first block in 2009,[112] and Bitcoin only achieved widespread attention in 2011,[113] it is unsurprising that so few cases exist concerning Bitcoin domestically and internationally. However, because of acceptance in the United States and abroad by many businesses and some governmental entities, and because no attempts have been made thus far by the government to intervene in an area where it has frequently intervened in the past, Bitcoin likely will be legal to own and use in the United States.[114]

IV. BITCOIN AND U.S. ANTI–MONEY LAUNDERING REGULATORY SCHEMES

A. Federal Law

Although Bitcoin is most likely a legal virtual currency, federal AML regulations may still apply when Bitcoin usage falls within regulation boundaries. Two categories effectively separate federal AML regulations: (1) prevention through regulatory measures and (2) punishment through criminal sanctions.[115] Prevention through regulation attempts to prevent dirty money from entering the U.S. financial system in the first place, and the Bank Secrecy Act and its

---

112. *See Genesis Block*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Genesis_block (last modified June 1, 2013) (the first block in the Bitcoin block chain).

113. Timothy B. Lee, *Bitcoin Implodes, Falls More than 90 Percent from June Peak*, ARS TECHNICA (Oct. 18, 2011, 12:45 PM), http://arstechnica.com/tech-policy/2011/10/bitcoin-implodes-down-more-than-90-percent-from-june-peak.

114. Another topic that warrants examination, which is beyond the scope of this Note, is whether Bitcoin is technically a legal currency or a legal commodity. A currency is "[a]n item (such as a coin, government note, or banknote) that circulates as a medium of exchange." BLACK'S LAW DICTIONARY, *supra* note 15, at 440. A commodity is "[an] article of trade or commerce . . . [that is] only tangible goods, such as products or merchandise, as distinguished from services . . . [or] [a]n economic good, esp. a raw material or an agricultural product." *Id.* at 310. Bitcoin seems to fall under both of these definitions in different ways (e.g., it does circulate as a medium of exchange; however, it also might be argued as a product "mined" from computational power). This determination may result in differing conclusions regarding under which regulatory schemes Bitcoin may fall.

115. *See* Shawn Turner, Note, *U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyberlaundering*, 54 CASE W. RES. L. REV. 1389, 1402–06 (2004); *see also* Grinberg, *supra* note 48, at 204–06 (discussing regulation and sanction means in relation to virtual currencies).

subsequent amendments represents the central pillar of this regulatory scheme.[116] Criminal sanctions, by contrast, attempt to disincentivize possible launderers through fines, imprisonment, or both, and to punish those who knowingly transact with money launderers.[117] The Money Laundering Control Act[118] is the primary vehicle for effecting criminal sanctions for money laundering, and some secondary vehicles include the prohibition of unlicensed money transmitting businesses provisions of 18 U.S.C. § 1960 and the bulk cash smuggling provisions of 31 U.S.C. § 5332.[119] Theoretically, the regulatory and criminal arms of AML policy act to detect and punish money laundering; however, the reach of these provisions to virtual currencies may be somewhat limited.

1. Regulatory Provisions and the Bank Secrecy Act

The United States' first legislative attempt to fight money laundering was the Bank Secrecy Act (BSA),[120] which established reporting requirements for institutions that might be used as money laundering vehicles.[121] The BSA effectively made certain institutions accountable for keeping records of transactions in excess of a $10,000 threshold when that institution might benefit from transaction and processing fees due to laundering activities.[122] These requirements gave investigators a paper trail to prosecute launderers and to find possible tax evaders.[123] However, launderers quickly began circumventing the BSA by breaking large transactions into smaller transactions of less than $10,000,[124] using financial service providers outside the scope of the BSA,[125] and using wire transfer systems to circumvent regulators until new regulations passed in 1995.[126]

After 1995, financial institutions required to record and report under the BSA included many nonbanking entities classified as money service businesses (MSBs).[127] After a refinement in 2011, this group includes:[128] (1) dealers in foreign

---

116. *See AML History*, *supra* note 3.

117. Turner, *supra* note 115, at 1405–06.

118. Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207-18 to -21 (1986) (codified as amended at 18 U.S.C. §§ 1956–57 (2006)).

119. *See* CHARLES DOYLE, CONG. RESEARCH SERV., RL33315, MONEY LAUNDERING: AN OVERVIEW OF 18 U.S.C. 1956 AND RELATED FEDERAL CRIMINAL LAW 36–39 (2012), *available at* http://www.fas.org/sgp/crs/misc/RL33315.pdf.

120. Turner, *supra* note 115, at 1402.

121. *Id.*

122. *Id.*

123. *See id.* at 1402–03.

124. *Id.* at 1403.

125. *Id.*

126. *See* Amendment to the Bank Secrecy Act Regulations Relating to Recordkeeping for Funds Transfers and Transmittals of Funds by Financial Institutions, 60 Fed. Reg. 220 (Jan. 3, 1995) (to be codified at 31 C.F.R. pt. 103) (establishing reporting requirements for transfers of U.S. $3000 or more); *see also* Turner, *supra* note 115, at 1403 (describing amendment proposal and effects).

127. Turner, *supra* note 115, at 1404.

128. *See* Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to

exchange, (2) check cashers, (3) issuers of traveler's checks or money orders, (4) providers of prepaid access, (5) money transmitters, (6) the U.S. Postal Service, and (7) sellers of prepaid access.[129] Finally, the 2001 USA PATRIOT Act ("Patriot Act")[130] extended the already broad definition of money transmitter.[131] This addition expanded the scope of the BSA from traditional financial institutions to nearly any person or business who facilitates money transfer.[132] The Patriot Act also extended the definition of financial institutions to include foreign banks and gave federal courts jurisdiction over some foreign-based money launderers.[133]

On March 18, 2013, FinCEN issued interpretive guidance for applying the BSA to virtual currencies.[134] This guidance came as a surprise to many, a welcome acknowledgement to some, and a harbinger of regulatory crackdown to others.[135] Overall, the guidance managed to clear up a few circulating questions, while also introducing a few new issues.

Interpreting from the composite BSA and subsequent amendments, the guidance begins by noting that FinCEN will not treat virtual currencies as equivalent to "real" currencies—that is, fiat currencies—even though the two share features.[136] FinCEN defined "real" currency as circulating legal tender of a country that is typically "used and accepted as a medium of exchange in the country of issuance";[137] however, no country accepts virtual currencies as a legal tender.[138] Further, the guidance noted that FinCEN would treat some users of virtual currencies as money transmitter MSBs, specifically defining roles of users, administrators, and exchangers,[139] but FinCEN will not consider virtual currency users as providers or sellers of prepaid access or dealers in foreign exchange.[140] The guidance does not discuss whether FinCEN would categorize Bitcoin users under the check casher, issuer of traveler's checks or money orders, or U.S. Postal Service MSB categories; however, it seems reasonable to assume that FinCEN

Prepaid Access, 76 Fed. Reg. 45404 (July 29, 2011) (codified as amended at 31 C.F.R. pts. 1010 and 1022).

129. 31 C.F.R. § 1010.100(ff) (2012) (defining "money services business").

130. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

131. *See id.* § 359(a), 115 Stat. at 328 (including as money transmitters "any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money").

132. Aside from simply including informal money transfer systems, the BSA also fails to define the phrase "as a business" and thus leaves a great deal of uncertainty. *See id.*

133. *Id.* § 377, 115 Stat. at 342 (extending 18 U.S.C. § 1029 to conduct committed abroad, so long as the tools or proceeds of the crimes pass through or are in the United States).

134. GUIDANCE, *supra* note 8, at 1.

135. *See* Jennifer Shasky Calvery, Dir., Fin. Crimes Enforcement Network, Remarks at United States Institute of Peace, The Virtual Economy: Potential, Perplexities and Promises 1 (June 13, 2013), *available at* http://www.fincen.gov/news_room/speech/pdf/20130613.pdf.

136. GUIDANCE, *supra* note 8, at 1.

137. *Id.* at 1 (citing 31 C.F.R. § 1010.100(m) (2012)).

138. *Id.*

139. *See id.* at 1–3.

140. *Id.* at 1, 5–6.

purposely omitted these categories due to their irrelevance. Thus, the guidance effectively pertains only to the money transmitter MSB category.

At the simplest level, the guidance defined a virtual currency user as "a person that obtains virtual currency to purchase goods or services."[141] Merely using virtual currency to purchase real or virtual goods or services will not transform a user into an MSB.[142] FinCEN arrived at this conclusion by reasoning that money transmitters must provide money transmission services, which means they must accept value from one person and transmit value to another location or person.[143] Plainly stated, a money transmitter is an intermediary between the buyer and seller. Therefore, a mere user does not engage in money transmission services.

However, once the user provides money transmission services, that user becomes a virtual currency exchanger, an administrator, or both.[144] The guidance defines an exchanger as "a person engaged *as a business* in the exchange of virtual currency for real currency, funds, or other virtual currency," and an administrator as "a person engaged *as a business* in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."[145] If an administrator or exchanger then "(1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason," that administrator or exchanger becomes a money transmitter under FinCEN's regulations and must comply with MSB requirements.[146] Although Bitcoin users, administrators, and exchangers fall under the "De-Centralized Virtual Currencies" section of the guidance,[147] the guidance muddies the waters when describing which entities fall under each of the three guidance-defined categories.

In keeping with the above guidance theme, users that merely use the virtual currency for real or virtual goods will not be subject to money transmitter regulation, even if that user created the virtual currency.[148] However, if the user sells virtual currency for "real currency or its equivalent," then that user becomes a money transmitter.[149] Further, if the user acts as an intermediary, accepting virtual currency from one user and transmitting it to another user during "the acceptance and transfer of currency, funds, or other value that substitutes for currency," then that user is both a money transmitter and an exchanger.[150] Thus, a miner who sells his or her bitcoins for a video game faces no regulation as an MSB, whereas a miner who sells a few bitcoins to a friend may be a money transmitter, and a Bitcoin exchange that transfers bitcoins and fiat currencies between users may be

141. *Id.*
142. *Id.* at 2–3.
143. *Id.* at 3. Interestingly, FinCEN makes no distinction for money transmitters between real or virtual currencies. *Id.*
144. *See id.* at 2–3.
145. *Id.* at 2 (emphasis added).
146. *Id.* at 3.
147. *See supra* note 67 and accompanying text.
148. GUIDANCE, *supra* note 8, at 5.
149. *Id.*
150. *Id.*

both a money transmitter and an exchange. Although this all seems relatively straightforward, certain questions arise.

As both exchanger and administrator definitions require the person to be acting "as a business,"[151] but never define what acting as a business entails, the guidance introduces uncertainty into the determination process. Imagine if a miner trades three hundred bitcoins—worth a net value of approximately $39,000—for a real good, such as a 2007 Porsche Cayman S.[152] Under current FinCEN guidance rules, this miner avoids MSB status. Conversely, when the same miner sells one bitcoin—assume a value of $130/BTC—to a friend for $5, the miner gains MSB status and faces regulation. However, when did the miner act as a business? Certainly, the $39,000 vehicle transaction seems more businesslike than sending a bitcoin to a friend at below market price. Similarly, imagine a Bitcoin exchange that allows users, at no charge, to only trade between several different virtual currencies. Such an exchange would cost the operator money to maintain in electricity and bandwidth, a net loss if he or she does nothing to monetize the exchange. Further, as the exchange only allows trading virtual currencies, money laundering of fiat currencies seems like a remote prospect. Yet the exchange operator faces regulation as both an exchanger and a money transmitter if FinCEN considers the exchange to be a business.

Given the apparent injustice of such scenarios, it seems appropriate for FinCEN to clarify its new definitions. This by no means implies that certain entities should not face regulation from FinCEN to combat money laundering that might occur on exchanges; however, the current definitions may result in unnecessarily tedious disputes over the definition of a business while continuing to allow money laundering through the sale of real goods.

2. Criminal Sanctions

a. Money Laundering Control Act

The Money Laundering Control Act of 1986 (MLCA)[153] made money laundering or knowingly assisting money laundering a federal crime.[154] The MLCA is broken down into two sections. The first section, codified at 18 U.S.C. § 1956, pertains to financial transactions involving the proceeds of certain other crimes,[155] either perpetrated or attempted,[156] known as "specified unlawful activit[ies]" (SUA).[157] The transaction must be accomplished (1) with the intent to promote SUA, (2) with the intent to evade taxation, (3) knowing the transaction is designed to conceal laundering, or (4) knowing the transaction is designed to avoid AML

151. *Id.* at 2.

152. *See* Mike Flacy, *Texas Family Sells Porsche – For 300 Bitcoins?*, DIGITAL TRENDS (Apr. 3, 2013), http://www.digitaltrends.com/cars/texas-family-sells-porsche-for-300-bitcoins.

153. Money Laundering Control Act of 1986, Pub. L. No. 99-579, 100 Stat. 3207-18 to -21 (1986) (codified as amended at 18 U.S.C. §§ 1956–57 (2006)).

154. Turner, *supra* note 115, at 1405 (citing 18 U.S.C. § 1956 (2006)).

155. 18 U.S.C. § 1956(a)(1) (2006).

156. *Id.* ("Whoever . . . conducts or attempts to conduct").

157. *Id.*; *see also id.* § 1956(c)(7) (defining "specified unlawful activity").

reporting requirements.[158] Additionally, anyone who attempts to or successfully "transports, transmits, or transfers . . . a monetary instrument or funds" into or from the United States from outside the United States, while meeting certain intent requirements, will also be guilty of money laundering.[159]

The second MLCA section, codified at 18 U.S.C. § 1957, goes beyond § 1956 by criminalizing monetary transactions greater than $10,000 derived from SUA.[160] A monetary transaction is a "deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument . . . by, through, or to a *financial institution*."[161] Although the defendant must know that the transaction involved criminally derived property,[162] no requirement exists that the defendant know of the tainting SUA;[163] thus, the defendant may not claim lack of knowledge of the SUA as a defense.[164] As long as the monetary transaction exceeded $10,000, involved criminally derived property from SUA, and involved a financial institution, then the defendant may be fined, imprisoned for up to ten years, or both.[165]

Applying the MLCA to Bitcoin, it may be difficult to prove § 1956 violations due to the knowledge or intent requirements.[166] However, because § 1957 has no such requirements, it would be easier to hold individuals accountable for tainted Bitcoin transfers. The overriding concern with either of these sections is that some SUA must be proven as a predicate offense and a person must be found to charge. In simple peer-to-peer transactions, where funds might be scattered among many Bitcoin addresses to hide the dirty money's source, tying any particular person to a pseudonymous account will prove extremely difficult. Even if a launderer uses a physical goods merchant that accepts Bitcoin payments to reintroduce cleansed money, and authorities can trace the transactions back to an original Bitcoin address, they would still need to tie that original Bitcoin address with a SUA. However, Bitcoin exchanges can be made resistant to such activity by requiring the exchange to identify both buyer and seller accounts, in line with AML requirements,[167] and then requiring the exchange to keep information about

158. *Id.* § 1956(a)(1)(A)(i)–(B)(ii).

159. *Id.* § 1956(a)(2).

160. *Id.* § 1957(a).

161. *Id.* § 1957(f)(1) (emphasis added) (defining "monetary transaction").

162. *Id.* § 1957(a).

163. *Id.* § 1957(c).

164. *See* United States v. Flores, 454 F.3d 149, 155 (3d Cir. 2006) ("[T]he defense's argument—that the Government needed to prove that Flores knew of, or was willfully blind to, the fact that the funds originated in drug trafficking to obtain a money laundering conviction—fails. *See* 18 U.S.C. § 1957(c) . . . .").

165. 18 U.S.C. § 1957(b).

166. That is, proving that the alleged money launderer possessed intent to promote SUA or to evade taxation, or knowingly concealed laundering or avoided AML reporting requirements, may prove difficult when Bitcoin allows users to be virtually anonymous.

167. 31 C.F.R. § 1010.312 (2012) ("[A] financial institution shall verify and record the name and address . . . identity, account number, and the social security or taxpayer identification number . . . ."). Mt. Gox, the world's largest Bitcoin exchange, announced on May 30, 2013, that all users wishing to deposit or withdraw currencies other than Bitcoin would need to become verified. Press Release, Mt. Gox Co. Ltd. Team, Statement Regarding

transactions and participants for five years. With these safeguards in place, authorities could be able to verify at least two parties in the chain of laundering. Although this is not a perfect solution, as it may not capture every step that a launderer may take to clean the dirty money, it may be as complete as can be achieved given the pseudonymous nature of Bitcoin.

b. Unlicensed Money Businesses

In addition to the MLCA, another avenue of pursuing money launderers is through 18 U.S.C. § 1960, which prohibits knowingly operating any part of an unlicensed money transmitting business (MTB).[168] According to 31 U.S.C. § 5330, a MTB includes any person or persons operating as an informal money transfer system outside of the conventional financial institutions system.[169] An unlicensed MTB is broadly defined as a MTB that affects interstate or foreign commerce to any degree[170] and that falls within one of three categories. The first category occurs when any MTB operates without a money-transmitting license within a state that requires licensure.[171] There is no requirement of knowledge that the MTB must be licensed;[172] however, the defendant must have known that he or she was operating a MTB and that his or her MTB was unlicensed.[173] The second category occurs when a MTB fails to comply with MTB registration requirements through the U.S. Department of the Treasury.[174] Again, the defendant must know that he or she is operating a MTB,[175] but he or she does not need to know the registration requirements.[176] Finally, the third category applies to a properly licensed MTB used to knowingly transmit or transport money that is derived from criminal activity or that is intended to finance criminal activity.[177]

Although Bitcoin almost certainly falls under the MTB definition because it is an informal money transfer system outside conventional financial institutions, there

---

Account Verifications (May 30, 2013), https://mtgox.com/press_release_20130530.html. Verification requires sending Mt. Gox multiple documents for authentication. Marion, *AML Account Statuses*, MT. GOX (May 31, 2013, 5:35 PM), https://support.mtgox.com/entries/21651045-AML-Account-Statuses.

168. 18 U.S.C. § 1960(a) (2006).

169. 31 U.S.C. § 5330(d)(1)(A) (2006).

170. 18 U.S.C. § 1960(b)(1).

171. *Id.* § 1960(b)(1)(A).

172. *Id.*

173. *E.g.*, United States v. Elfgeeh, 515 F.3d 100, 133 (2d Cir. 2008) ("We infer from the language of subsection (a) itself and from the absence from subsection (b)(1)(A) of a 'whether or not' clause mentioning knowledge of the possession of a license, that in order to convict under the amended § 1960(a), the government is required to prove that the defendant knew the money-transmitting business was unlicensed."); United States v. Talebnejad, 460 F.3d 563, 568 (4th Cir. 2006) ("The parties agree that the Government must allege and prove the defendant's knowledge [(1) that he operated a money transmitting business, (2) that it affected interstate commerce, and (3) that it was unlicensed under state law]."), *cert. denied*, 549 U.S. 1234 (2007).

174. *See* 18 U.S.C. § 1960(b)(1)(B).

175. United States v. Uddin, 365 F. Supp. 2d 825, 828–30 (E.D. Mich. 2005).

176. *See id.*; *see also Talebnejad*, 460 F.3d at 568.

177. 18 U.S.C. § 1960(b)(1)(C).

are several issues that might arise when trying to apply § 1960 to Bitcoin users and transactions. Under the first category—operating in a state without the required license—the user or service would have to know that they were in fact a MTB, and the state in which the operation occurred would need to require MTB licensure. Many average users would not necessarily know that sending money to another person would categorize them as a business, so proving knowledge may be difficult. Further, although most states today have state money transmitter laws,[178] there are still some that do not.[179] Failing to meet either of these elements would exclude Bitcoin transactions under the first category. Under the second category—operating without complying with Treasury Department regulations—registration is mandatory on a federal level;[180] however, the user still must know that he or she is a MTB, which may be difficult as discussed for the first category. Finally, under the third category—knowingly transmitting or transporting dirty money—licensure

---

178. *See* ALA. CODE §§ 8-7-1 to -15 (LexisNexis 2002 & Supp. 2012); ALASKA STAT. §§ 06.55.101–.107 (2012); ARIZ. REV. STAT. ANN. §§ 6-1201 to -1218 (2007); ARK. CODE ANN. §§ 23-55-101 to -1006 (2012); CAL. FIN. CODE §§ 2000–2153 (West 2013); COLO. REV. STAT. ANN. §§ 12-52-101 to -206 (West 2010 & Supp. 2012); CONN. GEN. STAT. ANN. §§ 36a-595 to -610 (West 2011); DEL. CODE ANN. tit. 5, §§ 2301–2318 (2001 & Supp. 2012); D.C. CODE §§ 26-1001 to -1027 (LexisNexis 2012); FLA. STAT. ANN. §§ 560.203–213 (West 2012); GA. CODE ANN. §§ 7-1-680 to -692 (2004 & Supp. 2013); HAW. REV. STAT. §§ 489D-1 to -34 (2008 & Supp. 2012); IDAHO CODE ANN. §§ 26-2901 to -2928 (2000 & Supp. 2013); 205 ILL. COMP. STAT. ANN. 657/1 to /105 (West 2007 & Supp. 2013); IND. CODE ANN. §§ 28-8-4-1 to -61 (West 2010 & Supp. 2012); IOWA CODE ANN. §§ 533C.101–.904 (West 2011 & Supp. 2013); KAN. STAT. ANN. §§ 9-508 to -513d (Supp. 2012); KY. REV. STAT. ANN. §§ 286.11-001 to -067 (LexisNexis 2012); LA. REV. STAT. ANN. §§ 6:1031–1053 (2005); ME. REV. STAT. ANN. tit. 32, §§ 6101–6146 (1999 & Supp. 2012); MD. CODE ANN., FIN. INST. §§ 12-401 to -431 (LexisNexis 2011 & Supp. 2012); MASS. ANN. LAWS ch. 169, §§ 1–16 (LexisNexis 2009 & Supp. 2013); MICH. COMP. LAWS ANN. §§ 487.1001–.1047 (West Supp. 2013); MINN. STAT. ANN. §§ 53B.01–.27 (West 2012 & Supp. 2013); MISS. CODE ANN. §§ 75-15-1 to -35 (Supp. 2011); MO. ANN. STAT. §§ 361.700–.729 (West 2000 & Supp. 2013); NEB. REV. STAT. ANN. §§ 8-1001 to -1019 (LexisNexis 2011); NEV. REV. STAT. ANN. §§ 671.010–.190 (LexisNexis 2009); N.H. REV. STAT. ANN. §§ 399-G:1 to :22 (Supp. 2012); N.J. STAT. ANN. §§ 17:15C-1 to -27 (West 2001); N.Y. BANKING LAW §§ 640 to 652-b (McKinney 2013); N.C. GEN. STAT. ANN. §§ 53-208.1 to .30 (West 2005 & Supp. 2012); N.D. CENT. CODE §§ 13-09-01 to -26 (2009 & Supp. 2013); OHIO REV. CODE ANN. §§ 1315.01–.19 (LexisNexis 2012); OKLA. STAT. ANN. tit. 6, §§ 1511–1515 (West Supp. 2013); OR. REV. STAT. §§ 717.200–.905 (2011); 7 PA. CONS. STAT. ANN. §§ 6101–6122 (West 1995 & Supp. 2013); R.I. GEN. LAWS §§ 19-14-1 to -14-33 (Supp. 2012); S.D. CODIFIED LAWS §§ 51A-17-1 to -47 (Supp. 2013); TENN. CODE ANN. §§ 45-7-201 to -229 (Supp. 2013); TEX. FIN. CODE ANN. §§ 151.301–.309 (West 2013); UTAH CODE ANN. §§ 7-1-501 to -508 (LexisNexis 1995 & Supp. 2013); VT. STAT. ANN. tit. 8, §§ 2500–2561 (2009 & Supp. 2012); VA. CODE ANN. §§ 6.2-1900 to -1921 (2010 & Supp. 2013); WASH. REV. CODE ANN. §§ 19.230.005–.905 (West 2013); W. VA. CODE ANN. §§ 32A-2-1 to -28 (LexisNexis 2011); WIS. STAT. ANN. §§ 217.01–.21 (West 2009); WYO. STAT. ANN. §§ 40-22-101 to -129 (2013).

179. Montana, South Carolina, and New Mexico do not have state money transmitter laws. A similar New Mexico statute applies only to checks and money orders, not money transmissions. *See* N.M. STAT. ANN. § 58-20-1 (West 2003).

180. 31 U.S.C. § 5330(a)(1) (2006).

is a nonissue, but the MTB must knowingly transmit or transport dirty money. This category again suffers from a knowledge requirement, and innocent transmitters, who have no knowledge of a transaction's tainted status, are likely to be excluded under this category.

The best chance for holding a prospective MTB in violation of 18 U.S.C. § 1960 occurs either when the individual knows that he or she functions as a MTB, and therefore would qualify under the second category (and also under the first category if the state requires money transmitters to register with the state). An alternative avenue exists when the individual clearly knows the transactions involve dirty money, thus qualifying under the third category. Setting category three aside, as additional evidence would be needed to support the underlying criminal offense, Bitcoin exchanges are in the best position to understand their role as a MTB. An exchange operates as an intermediary between buyer and seller by its very design, and even the most ignorant exchange could probably be held liable for willful blindness given the circumstances surrounding their activities.[181]

In fact, on May 14, 2013, Magistrate Judge Susan Gauvey signed a seizure warrant for the contents of an account used by Mt. Gox, the largest Bitcoin exchange in the world, pursuant to 18 U.S.C. § 1960 for Mt. Gox's failure to register as a money transmitter with either the federal government or any state government.[182] The supporting affidavit established probable cause to believe that Mt. Gox operated an account as an unlicensed money transmitter business and noted that Mt. Gox completed a form indicating that it did not act as a money transmitter.[183] However, even if prosecutors were unable to prove actual knowledge, they may be able to show that Mt. Gox was willfully blind of its position given the nature and size of the exchange.[184]

3. Federal Law Summary

Federal AML efforts may impose regulations or criminally punish some Bitcoin users. Under the BSA and FinCEN's recent guidance for virtual currencies, those who exchange bitcoins for fiat currency or act as intermediaries to virtual currency transactions may be subject to regulations. Punishment under the MLCA may be possible if the underlying SUA can be proven. Finally, punishment under 18 U.S.C. § 1960 will be most effective where knowledge of a licensure requirement can be shown or if the money is clearly dirty. In all of these categories, exchanges will be the most likely candidates for action.

---

181. *Cf.* United States v. Schnabel, 939 F.2d 197, 203 (4th Cir. 1991) ("The willful blindness instruction allows the jury to impute the element of knowledge to the defendant if the evidence indicates that he purposely closed his eyes to avoid knowing what was taking place around him.").

182. Application and Affidavit for Seizure Warrant, *In re* the Seizure of the Contents of One Dwolla Account, No. 1:13-mj-01162-SKG (D. Md. May 28, 2013).

183. Affidavit in Support of Seizure Warrant at 2–4, *In re* the Seizure of the Contents of One Dwolla Account, No. 1:13-mj-01162-SKG (D. Md. May 28, 2013).

184. *See Schnabel*, 939 F.2d at 203–04; *see also* text accompanying *supra* note 181.

B. State Law

1. Uniform Money Services Act

In addition to federal AML laws, many states have also passed laws that could regulate Bitcoin money laundering. In 2000, the National Conference of Commissioners on Uniform State Laws (NCCUSL) developed the Uniform Money Services Act (UMSA) in an attempt to create a cohesive set of state laws to effectively regulate MSBs.[185] Theoretically, the UMSA's adoption by the states would establish clear, consistent licensure requirements.[186]

The UMSA defines MSBs as nonbank entities that provide alternative payment or exchange mechanisms, distinct from traditional banks or financial institutions.[187] The UMSA also creates three categories of licensees: (1) money transmission services,[188] which may also perform check cashing and currency exchange; (2) check cashers,[189] which may also perform currency exchange; and (3) currency exchanges,[190] which may only perform currency exchange.[191] However, because money transmission services encapsulate both lower categories, money transmission services are subject to comparatively greater application and security requirements.[192]

To accommodate new Internet-based transaction schemes, the UMSA broadens the definition of money to "monetary value," which includes "a medium of exchange, whether or not redeemable in money."[193] Internet payment and stored-value schemes are then broken down into several categories including (1) stored

---

185. *See* UNIF. MONEY SERVS. ACT pref. n.A (amended 2013), 7A Pt. III U.L.A. 163 (2006). Alaska, Arkansas, Iowa, Puerto Rico, Texas, U.S. Virgin Islands, Vermont, and Washington have adopted the UMSA. *Legislative Fact Sheet—Money Services Act*, UNIF. LAW COMMISSION, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Money%20Services%20Act.

186. UNIF. MONEY SERVS. ACT pref. n.A.

187. *Id.* at pref. n.B(1).

188. *Id.* § 102(14).

189. *Id.* § 102(4).

190. *Id.* § 102(6) ("'Currency exchange' means receipt of revenues from the exchange of money of one government for money of another government.").

191. *See id.* at pref. n.C.

192. *Compare id.* §§ 202–03, *with id.* §§ 302, 402. "[C]heck cashers [under § 302] and currency exchangers [under § 402] are subject to different types of reporting and record-keeping requirements [than money transmitters under §§ 202–03] and similarly are exempt from bond and net worth requirements." *Id.* at pref. n.C. The UMSA drafters explained this difference in treatment to be reasonable because "check cashers and currency exchangers do not accept funds from consumers for obligations that might remain unpaid. Rather, both check cashers and currency exchangers immediately provide customers with funds. There is no risk that customers may lose their money (unlike the risk posed by purchasing a money order that might not be redeemed)." *Id.*

193. *Id.* § 102(11); *id.* at cmt. 10.

value,[194] (2) E-money and Internet payment mechanisms,[195] (3) Internet scrip,[196] (4) Internet funds transfer,[197] (5) gold or precious metals transfer and payment,[198] and (6) Internet bill payment services.[199] For the UMSA to apply, Bitcoin would first need to fall within the definition of a medium with monetary value.

Bitcoin will fall into the above UMSA definition, as it can be a medium of exchange for Bitcoin users, merchants, and Bitcoin exchanges. Additionally, Bitcoin likely falls into one or more Internet payment and stored-value scheme categories. Further, Bitcoin may be a stored value because all Bitcoin transactions and balances exist in the decentralized, public record. Bitcoin also serves as a token or notational system, as all bitcoins are essentially encoded data strings that serve as cash substitutes. Additionally, bitcoins may act like scrip because they are a form of alternative value exchanged over the Internet; however, it may be difficult to call bitcoins coupons or bonus points instead of a virtual currency in and of itself.[200] Finally, bitcoins most likely will not fall under the remaining terms because Bitcoin is not money accepted by any government, does not involve precious metals, and does not function as an automated bill payment intermediary. Thus, bitcoins have monetary value as (1) stored value, (2) a token e-money, or (3) a scrip.

---

194. *See id.* § 102(21) ("'Stored value' means monetary value that is evidenced by an electronic record.").

195. E-money refers to "money or a money substitute" stored on a computer device for transfer over information systems. *Id.* at pref. n.D(2). E-money is further broken down into two categories: (1) traditional payment mechanisms (e.g., ACH), where the Internet serves only as a communication channel; and (2) Internet payment mechanisms involving E-money. Internet-based E-money systems further break down into two categories: (1) token or notational systems, where electronic tokens (represented as numbers or symbols) are purchased from an issuer and serve as cash substitutes to merchants, which then redeem value from the issuer; and (2) account-based systems, where the consumer purchases E-money by withdrawing value from a bank or credit card account and the E-money issuer stores this value for a merchant to withdraw. *Id.*

196. Scrip refers to value exchanged over the Internet but not redeemable for money, analogous to coupons or bonus points which may be exchanged for goods or services but which have no cash value. *Id.* at pref. n.D(3).

197. These are "[n]ew payment services offered by banks and nonbanks [that] will transfer money over the Internet." *Id.* at pref. n.D(4). Here, money refers to a medium of exchange authorized or adopted by the United States, a foreign government, or both. *Id.* § 102(12) (defining "money").

198. *Id.* at pref. n.D(5).

199. *Id.* at pref. n.D(6).

200. A coupon is "[a]n interest or dividend certificate that is attached to another instrument, such as a bond, and that may be detached and separately presented for payment of a definite sum at a specified time." BLACK'S LAW DICTIONARY, *supra* note 15, at 404. Bitcoins, however, are not attached to another instrument, as they may be traded on their own on an exchange or between two users. *See, e.g.*, LOCAL BITCOINS.COM, https://localbitcoins.com. Bitcoins also do not necessarily represent a definite sum due to constant fluctuation in value. *See* Lee, *supra* note 113. Bonus points are given by merchants to customers as patronage rewards, redeemable through the merchant for some other good or prepaid value card. *See, e.g.*, MYPOINTS, https://www.mypoints.com. Conversely, bitcoins would instead be a reward offered on redemption of bonus points.

Next, the licensee hierarchy under which to classify Bitcoin must be determined. Categorizing peer-to-peer Bitcoin transactions under the most regulated category, money transmission services, is difficult because the definition of money transmission excludes intermediary entities that merely act as transaction clearing agents, provide delivery services, or act as data transmission channels.[201] In a simple peer-to-peer transfer, the Bitcoin protocol and the miners who complete blocks act as the intermediary entities largely excluded under the definition. Conversely, the money transmission does include "Internet payment services that hold customer's funds or monetary value for their own account rather than serve simply as clearing agents."[202] This most likely would include Bitcoin currency exchanges, which can hold value from both buyers and sellers for trades. Thus, Bitcoin exchanges might fall within the more rigorous requirements of the first category, but simple transactions between peers may not.

The second category, check cashing, also has strained relevance to Bitcoin. The comments to the UMSA note that check-cashing entities must collect a fee in consideration for their provided check cashing service.[203] Although the Bitcoin network has in place arbitrary minimum transaction fees that a sender pays,[204] there is no fee actually necessary for a transaction to be included in a completed block.[205] Further, the individual who completes the block receives the fees collected, not the sending or receiving parties.[206] Thus, neither party necessarily generates a fee in the peer-to-peer transfer nor is a fee necessarily collected from the transfer if the sender does not specify such a fee. Check cashing might apply to a Bitcoin exchange that takes some amount of the transaction as payment for its service;[207] however, without such a fee, the transaction does not meet the definitional requirements for check cashing.

Finally, categorizing Bitcoin under the third category, currency exchange, is difficult. This is primarily due to the definition as "the exchange of money of one government for money of another government."[208] No government accepts bitcoins as an official form of money, and therefore it is unclear how such a definition would ever include a non-government-backed currency of any kind.

---

201. UNIF. MONEY SERVS. ACT § 102 cmt. 9 (discussing the definition of "money transmission").

202. *Id.*

203. *Id.* § 102 cmt. 3.

204. *Transaction Fees*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Transaction_fees (last modified Aug. 31, 2013).

205. *See id.*; *see also Free Transaction Relay Policy*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Free_transaction_relay_policy (last modified Oct. 18, 2012) (describing an alternative mode of accepting bitcoins that does not filter "unacceptable" transactions like the standard Bitcoin client).

206. *See Transaction Fees*, supra note 204.

207. *See, e.g.*, Adam, *Step 3—Buying or Selling Bitcoins*, MT. GOX (July 21, 2011, 4:03 PM), http://support.mtgox.com/entries/20294238-step-3-buying-or-selling-bitcoins ("Please note that our ordering system currently subtracts the trade fee from the 'Total' when the order is processed.").

208. UNIF. MONEY SERVS. ACT § 102(6) (defining "currency exchange").

2. California

The 2010 California Money Transmission Act ("California Act") defines a money transmission as "(1) [s]elling or issuing payment instruments[,] (2) [s]elling or issuing stored value[, or] (3) [r]eceiving money for transmission."[209] When asked what the California Act encompassed, a spokesperson stated, in agreement with the earlier simplification in this Note,[210] that the California Department of Financial Institutions uses a plain-English test: "'Do you take funds/value from A and agree to pay them to B on behalf of A; and/or Do you take funds/value from A, and store it so that A can make purchases from third parties or take cash out at a later date.'"[211] Unsurprisingly, critics accuse the law's broad language of chilling innovation.[212] Many payment technology startups hold money for some period or act as a payment intermediary between buyers and sellers.[213] Forcing these companies, which may be cash-strapped already, to pay the required surety bonds of at least $500,000 or 50% of average daily outstanding payment instrument and stored value obligations[214] may prove disastrous for the company's survival.

However, it is unlikely that a peer-to-peer Bitcoin transfer will qualify under this plain-English test. If A is the buyer and B is the seller, then whom is the person or company holding the funds during the transfer? In a simple peer-to-peer transfer, no entity holds the funds during the transfer; the network simply sees a broadcast of information deducting one Bitcoin address of a set amount of bitcoins and crediting another Bitcoin address with that same amount of bitcoins. This is not the case with a Bitcoin currency exchange, which can hold fiat currencies or bitcoins on behalf of a user, or perhaps some sort of Bitcoin proxy payment service that a money launderer might use to obfuscate dirty money's origins.[215] Nevertheless, the fact remains that the California Act is not written in a way that would include all Bitcoin transactions, and the plain-English test stated by the California Act's officiating body supports this conclusion.

---

209. CAL. FIN. CODE § 2003(o)(1)–(3) (West 2013).

210. *See supra* text accompanying note 144 ("Plainly stated, a money transmitter is an intermediary between the buyer and seller.").

211. Owen Thomas, *This Innovation-Killing California Law Could Get a Host of Startups in Money Trouble*, BUS. INSIDER (July 11, 2012, 6:21 PM), http://www.businessinsider.com/california-money-transmitter-act-startups-2012-7.

212. *See id.*; *see also* Aaron Greenspan, *In Fifty Days, Payments Innovation Will Stop in Silicon Valley*, QUORA (May 11, 2011), https://www.quora.com/Aaron-Greenspan/Posts/In-Fifty-Days-Payments-Innovation-Will-Stop-In-Silicon-Valley; James Mariani, *The California Money Transmission Act: Boon to Consumers or Bane to Innovation?*, U. ILL. J.L. TECH. & POL'Y TIMELY TECH, (Sept. 26, 2012), http://illinoisjltp.com/timelytech/hello-world/.

213. *See, e.g.*, *iTunes*, APPLE, https://www.apple.com/itunes/what-is/#store; *Google Play*, GOOGLE, https://play.google.com/store; *FAQ*, KICKSTARTER, http://www.kickstarter.com/help/faq/kickstarter%20basics.

214. CAL. FIN. CODE § 2037(d).

215. *See, e.g.*, BITLAUNDRY, http://app.bitlaundry.com.

3. Virginia

The Virginia Money Order Sellers and Money Transmitters ("Virginia Act") provision of the Virginia Code[216] defines "money transmission" as "receiving money or monetary value for transmission by wire, facsimile, electronic means or other means or selling or issuing stored value."[217] It also defines "monetary value" as "a medium of exchange, whether or not redeemable in money";[218] and defines "stored value" as "monetary value that is evidenced by an electronic record."[219] The Virginia Act requires a license for any person engaged in selling money or in the business of money transmission,[220] a surety bond of between $25,000 and $1 million that can remain in effect for five years after licensee ceases activity,[221] a $750 annual renewal fee,[222] and retention of records for at least three years.[223] The Virginia Act also imposes a civil penalty of a fine up to $2500 and a criminal penalty of a class one misdemeanor for any persons that act as money transmitters without proper licensure.[224]

The Virginia Act applies more readily to Bitcoin than does the California Act. The first part of the money transmission, according to the Virginia Act, requires "*receiving* money or monetary value *for transmission*."[225] This indicates value came from a sending party, went to a money transmitter, and is awaiting transmission to a final receiving party. Thus, a money transmitter under the Virginia Act is essentially the same as a money transmitter under the California Act, and a simple peer-to-peer Bitcoin transaction has no such intermediary. However, the second part of the definition includes "selling or issuing stored value."[226] Because a stored value is any medium of exchange that is electronically recorded, which does not need to actually be redeemable, it would likely capture Bitcoin within its definition. Bitcoin is publicly recorded as a block chain, does not necessarily have to be redeemed, and can act as a medium of exchange for Bitcoin users as evidenced by the individuals and organizations that accept it.

Virginia validated these assumptions, at least partially, on May 31, 2013, when Tangible Cryptography, LLC, received notice from the Commonwealth of Virginia that the company might be operating as an unlicensed money transmitter in the state, despite being registered with FinCEN as an MSB.[227] Thus, the company violated the state requirement for licensure while fulfilling the federal requirement. The company suspended its operations pending further review, but the ordeal raises

---

216. VA. CODE ANN. §§ 6.2-1900 to -1921 (2010 & Supp. 2013).
217. *Id.* § 6.2-1900.
218. *Id.*
219. *Id.*
220. *Id.* § 6.2-1901.
221. *Id.* § 6.2-1904.
222. *Id.* § 6.2-1905.
223. *Id.* § 6.2-1916.
224. *Id.* §§ 6.2-1920 to -1921.
225. *Id.* § 6.2-1900 (emphasis added).
226. *Id.*
227. *See* Johann Summers, *FastCash4Bitcoins Suspends Sales*, BITCOIN MAG. (June 3, 2013), http://bitcoinmagazine.com/fastcash4bitcoins-suspends-sales.

questions about the difficulties of compliance with disparate federal and state laws in addition to the general lack of clarity resulting from FinCEN's guidance.[228]

The differing status of Bitcoin between Virginia and California state laws is largely one of definition. Although the California Act is broadly worded, it fails to capture transmissions outside of intermediaries. The Virginia Act, however, includes both intermediaries and those simply selling or issuing stored value. Virginia codified the Virginia Act in 1974 and subsequently modified it five times.[229] California passed the California Act 2010, combining preexisting California licensing schemes and expanding licensing to new technologies and domestic transmissions.[230] Therefore, the failure to include Bitcoin-like technologies in the California Act may have merely been an oversight in drafting that will be remedied in future revisions. In essence, the Virginia Code may simply be more mature and refined than the California Act.[231]

4. State Law Summary

Similar to federal regulation schemes, where an entity falls within the Bitcoin transaction largely determines whether that entity will face enforcement under state laws. The UMSA will likely exclude simple peer-to-peer Bitcoin transactions from regulation. Although Bitcoin probably falls within the definition of monetary value for the UMSA, it most likely will fall outside the three categories for licensing. The only real exception to this may be Bitcoin currency exchanges, which probably would fall into at least one of the licensing schemes.

V. GOING FORWARD: WHOM TO REGULATE?

Regulation of the Bitcoin network will be difficult because of its complex and decentralized nature, which renders it essentially impervious to a single point of failure. Instead of trying to control all aspects of the Bitcoin network, it is more effective to analyze each Bitcoin transaction entity individually and determine in an abbreviated cost-benefit analysis what will be the best aspects to regulate. As previously shown, regulation of the Bitcoin transaction largely depends upon the targeted regulation entity, further enforcing this entity-by-entity analysis.

A. Sender

Regulating the initial Bitcoin sender will likely prove unfeasible due to the largely pseudonymous and dispersed nature of senders' identities in the Bitcoin network. When a sender simply sends bitcoins to another average Bitcoin user or to a money laundering service, no personally identifiable information (PII) is interchanged. Unless there is some physical or traceable output from the transaction

---

228. *Id.*
229. *See* VA. CODE ANN. § 6.2-1900.
230. *See* Mariani, *supra* note 212.
231. Thanks to Professor Sarah Jane Hughes for this comparison. Interview with Sarah Jane Hughes, Univ. Scholar & Fellow in Commercial Law, Maurer School of Law, in Bloomington, Ind. (Mar. 26, 2013).

(e.g., the sender supplied his shipping address), the likelihood of identifying the owner of a one-time-use Bitcoin address is extremely low. Further, attacking a community's user base will likely result in greater distrust and disapproval toward government, a key reason Bitcoin was established,[232] and could lead to increased anonymization.[233] Thus, the input of resources to attempt to track users that have not provided any PII greatly outweighs the benefit of regulating what are likely to be minor transactions and may possibly result in even greater obfuscation of money laundering.

B. Launderer

Similarly, regulating the Bitcoin receivers or launderers will be unfeasible. Although this could allow for targeted enforcement and regulation of those acting with clear criminal intent (e.g., blatant money launderers) and avoid the community backlash that might result from attempting to regulate all Bitcoin senders, regulation of launderers faces the same issues of anonymity. If there is no physical output or PII to trace, law enforcement will devote significant resources for relatively small rewards. Additionally, many blatant infringers may hide behind less rigorous international laws and avoid U.S. regulations while openly promoting criminal activities. Thus, going after Bitcoin receivers in general, and money launderers specifically, will prove inefficient.

C. Processors

Although Bitcoin processors (miners) more readily fit within current regulatory schemes, they would prove unreasonably difficult to regulate. Miners effectively take the place of a payment processor, including possibly taking a small fee in return for their work, but there is no actual requirement for such a fee in Bitcoin transactions.[234] Further, a certain lack of mens rea culpability exists when processing the transaction, as the mining software processes transactions for the block without user intervention. Although some Bitcoin users may understand how the Bitcoin network operates and how their mining activity may complete a block of transactions, the majority of users may simply be incentivized by the possibility of rewards.

Although there may be a reasonable probability of proving willful blindness, it may still be unwise to pursue Bitcoin miners individually. Even though each block rewards the successful miner, and that miner's Bitcoin address is recorded in the

---

232. *See* Jeffries, *supra* note 90; *see also supra* text accompanying note 101.

233. This could occur through many established and emerging anonymization protocols. *See, e.g.*, *Tor: Overview*, TOR PROJECT, https://www.torproject.org/about/overview.html; I2P ANONYMOUS NETWORK, http://www.i2p2.de; *see also* Adrian Chen, *'Dark Net' Kiddie Porn Website Stymies FBI Investigation*, GAWKER (June 11, 2012, 12:02 PM), http://gawker.com/5916994/dark-net-kiddie-porn-website-stymies-fbi-investigation; Sean Gallagher, *Anonymous Takes Down Darknet Child Porn Site on Tor Network*, ARS TECHNICA (Oct. 23, 2011, 7:00 PM), http://arstechnica.com/business/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network.

234. *See supra* notes 204–06 and accompanying text.

public Bitcoin record, a miner is still pseudonymous. The possibility of further fracturing and obfuscating the Bitcoin network, as in the above two scenarios, means pursuing Bitcoin miners is also inefficient and possibly detrimental.

D. Bitcoin Development Team

Although regulating the Bitcoin development team might seem like an efficient attack on a central authority figure that would prevent the Bitcoin network from uniformly reacting to challenges faced by Bitcoin, this assumption fails to recognize the reality of Bitcoin as an open-source software[235] with an active community. Because the Bitcoin code is open-source,[236] distributed to all those who wish to inspect it,[237] stopping the development team would not actually stop distribution of the code. At most, it would temporarily delay code updates until another group of individuals took over code updates, probably in a more secretive manner instead of the publicly known group[238] that operates today.

Additionally, it would be hard to say that the Bitcoin development team has any actual input on the individual transactions that may occur on the network. The development team acts more as a standards agency,[239] rather than as a central authority that controls the operation of the network. Thus, although the Bitcoin development team would be a known target, and thus easier to personally prosecute, it is questionable whether removing their influence on the network would serve to lessen illegal activity that might occur through Bitcoin.

E. Currency Exchanges

Finally, and most promising, is the regulation of Bitcoin currency exchanges. Because Bitcoin exchanges usually deal with fiat currencies, they will more readily fall under money exchange laws that define money as currency backed by a government. Additionally, because they can hold value from buyers and sellers for transactions, they should easily be classified as money transmitters—that is, intermediaries between a buyer and a seller—under money transmitter laws. Further, exchanges gain credibility through user confidence and volume. If the

---

235. Open-source software is "[s]oftware that is [usually] not sold for profit, includes both human-readable source code and machine-readable object code, and allows users to freely copy, modify, or distribute the software." BLACK'S LAW DICTIONARY, *supra* note 15, at 1200.

236. BITCOIN PROJECT, *supra* note 13 ("Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part.") (emphasis omitted).

237. *See Bitcoin*, SOURCEFORGE, http://sourceforge.net/projects/bitcoin/files/Bitcoin.

238. *See People*, BITCOIN WIKI, https://en.bitcoin.it/wiki/People (last modified June 13, 2013) (giving a more expansive list of individuals involved in the Bitcoin project).

239. *See, e.g.*, *Frequently Asked Questions*, BITCOIN PROJECT, http://bitcoin.org/en/faq ("While developers are improving the software, they can't force a change in the Bitcoin protocol because all users are free to choose what software and version they use. In order to stay compatible with each other, all users need to use software complying with the same rules. Bitcoin can only work correctly with a complete consensus among all users. Therefore, all users and developers have a strong incentive to protect this consensus.").

exchange has few users willing to trade or if the exchange is not trustworthy, it will not easily allow the stages of money laundering to occur without attracting attention. Due to this tradeoff, exchanges are likely to be less decentralized, and therefore will be easier to target for regulation. An exchange that facilitates hundreds or thousands of transactions, possibly receiving fees for processing the transactions, will fail to prove a legitimate lack of knowledge, as it is unreasonable that its activity would go unregulated while similar payment exchanges are subject to state, federal, and international money exchange and transmission laws. Therefore, out of the core entities of a Bitcoin transaction, regulation of Bitcoin currency exchanges seems likely to have the greatest effect for the least investment of resources.

CONCLUSION

Bitcoin represents a disruptive financial technology that many AML and money transmitter statutes are ill prepared to deal with. Virtual currencies in general have broken the trend of physical, government-backed coin and paper currencies, and it is unlikely that any new law will capture all iterations of emerging technologies for any significant period. But this does not mean that Bitcoin and similar virtual currencies should be deemed illegal or should be onerously regulated to compensate for the lack of initial oversight. In an increasingly digital world, it makes perfect economic and societal sense to allow digital currencies, government-backed or otherwise.

Regulation of such currencies should occur at the point where law enforcement can most effectively punish civil and criminal violations with the least overhead. Because Bitcoin is a decentralized, peer-to-peer virtual currency, it makes little since to regulate entities other than Bitcoin currency exchanges. Increased pressure on users will only serve to increase the cost of enforcement in the long run. Some Bitcoin currency exchanges have already shown initiative by registering as MSBs under current AML schemes.[240] Instead of increasing regulation and trying to predict the next generation of disruptive technologies, it would ultimately be better to understand the technologies and police the points of public contact with existing legal schemes.

240. *See e.g.*, *MSB Registrant Search Web Page*, FINCEN, http://www.fincen.gov/financial_institutions/msb/msbstateselector.html (Mt. Gox registered as MSB Registration Number/DCN: 31000029348132; Bitfloor registered as MSB Registration Number/DCN: 31000005224108; BitInstant registered as MSB Registration Number/DCN: 31000005031107).

Toronto Academe Press

9 780973 981315 >